MaxiiNet™ VI3010
Operational Manual

10 Port Series PoE+ L2 Plus Managed Switch
Release V1.00

© 2014 Vigitron, Inc. All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies.

About This Manual

Copyright

Copyright © 2014 Vigitron, Inc. All rights reserved. The products and programs described in this user's manual are licensed products of Vigitron, Inc. This user's manual contains proprietary information protected by copyright, and this user's manual and all accompanying hardware, software and documentation are copyrighted. No parts of this user's manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from by any means electronic or mechanical. This also Includes photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Vigitron, Inc.

Purpose

This manual gives specific information on how to operate and use the management functions of the Vi3010.

Audience

The manual is intended for use by network administrators who are responsible for operating and maintaining network equipment. Consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions

The following conventions are used throughout this manual to show information.

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to a potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warranty

See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to Vigitron's products and replacement parts can be obtained from Vigitron's Sales and Service Office or an authorized dealer.

Disclaimer

Vigitron does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Vigitron disclaims liability for any inaccuracies or omissions that may have occurred. Information in this user's manual is subject to change without notice and does not represent a commitment on the part of Vigitron. Vigitron assumes no responsibility for any inaccuracies that may be contained in this user's manual. Vigitron makes no commitment to update or keep current the information in this user's manual, and reserves the rights to make improvements to this user's manual and/or to the products described in this user's manual, at any time without notice.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Caution

To assure continued compliance (example-use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class B device. In a domestic environment, this product may cause radio interference. In which case, the user may be required to take adequate measures.

UL Mark

Ul 60950-1 Information Technology Equipment - Safety - Part 1: General Requirements - Edition 2 - Revision Date 2014/05/13

Contents

About This Manual....1
Introduction....8
Chapter 1: Operation of Web-Based Management....9
Chapter 2: System Configuration....11
2-1 System Information....11
2-1.1 Information....11
2-1.2 Configuration....13
2-2 Time....14
2-2.1 Manual....14
2-2.2 NTP....16
2-3 Account....17
2-3.1 Users....17
2-3.2 Privilege Level....19
2-4 IP....21
2-4.1 IPV4....21
2-4.2 IPV6....23
2-5 Syslog....24
2-5.1 Configuration....24
2-5.2 Log....25
2-5.3 Detailed Log....26
2-6 SNMP....27
2-6.1 System....27
2-6.2 Configuration....28
2-6.3 Communities....29
2-6.4 Users....30
2-6.5 Groups....32
2-6.6 Views....33
2-6.7 Access....34
2-6.8 Trap....36
Chapter 3: Configuration....38
3-1 Port....38
3-1.1 Configuration....38
3-1.2 Port Description....40
3-1.3 Traffic Overview....41
3-1.4 Detailed Statistics....42
3-1.5 QoS Statistics....44
3-1.6 SFP Information....45
3-1.7 EEE....47

3-2 ACL 49
3-2.1 Ports 49
3-2.2 Rate Limiters 51
3-2.3 Access Control List 52
3-2.4 ACL Status 55
3-3 Aggregation 57
3-3.1 Static Trunk 57
3-3.2 LACP 59
3-4 Spanning Tree 64
3-4.1 Bride Settings 64
3-4.2 MSTI Mapping 67
3-4.3 MSTI Priorities 69
3-4.4 CIST Ports 70
3-4.5 MSTI Ports 72
3-4.6 Bridge Status 74
3-4.7 Port Status 75
3-4.8 Port Statistics 76
3-5 IGMP Snooping 77
3-5.1 Basic Configuration 77
3-5.2 VLAN Configuration 79
3-5.3 Port Group Filtering 81
3-5.4 Status 83
3-5.5 Group Information 84
3-5.6 IPV4 SSM Information 85
3-6 MLD Snooping 87
3-6.1 Basic Configuration 87
3-6.2 VLAN Configuration 90
3-6.3 Port Group Filtering 92
3-6.4 Status 93
3-6.5 Group Information 94
3-6.6 IPV6 SSM Information 95
3-7 MVR 96
3-7.1 Configuration 96
3-7.2 Port Group Allow 98
3-7.3 Groups Information 99
3-7.4 Statistics 100
3-8 LLDP 101
3-8.1 LLDP Configuration 101
3-8.2 LLDP Neighbors 104
3-8.3 LLDP-MED Configuration 106

3-8.4 LLDP-MED Neighbors 112
3-8.5 EEE 115
3-8.6 Port Statistics 117
3-9 PoE 119
3-9.1 Configuration 119
3-9.2 Status 121
3-9.3 Power Delay 123
3-9.4 Auto Checking 124
3-9.5 Scheduling 126
3-10 Filtering Data Base 127
3-10.1 Configuration 127
3-10.2 Dynamic MAC Table 130
3-11 VLAN 131
3-11.1 VLAN Membership 131
3-11.2 Ports 133
3-11.3 Switch Status 135
3-11.4 Port Status 137
3-11.5 Private VLANs 139
3-11.6 MAC-Based VLAN 141
3-11.6.1 Configuration 141
3-11.7 Protocol-Based VLAN 144
3-12 Voice VLAN 149
3-12.1 Configuration 149
3-12.2 OUI 151
3-13 GARP 152
3-13.1 Configuration 152
3-13.2 Statistics 154
3-14 GVRP 155
3-14.1 Configuration 155
3-14.2 Statistics 157
3-15 QoS 158
3-15.1 Port Classification 158
3-15.2 Port Policing 160
3-15.3 Port Schedulers 161
3-15.4 Port Shaping 163
3-15.5 Port Tag Remarking 166
3-15.6 Port DSCP 167
3-15.7 DSCP-Based QoS 169
3-15.8 DSCP Translation 170
3-15.9 DSCP Classification 172

3-15.10 QoS Control List Configuration 173
3-15.11 QCL Status 177
3-15.12 Storm Control 179
3-16 S-Flow Agent 180
3-16.1 Collector 180
3-16.2 Sampler 182
3-17 Loop Protection 184
3-17.1 Configuration 184
3-17.2 Status 186
3-18 Single IP 187
3-18.1 Configuration 187
3-18.2 Information 188
3-19 Easy Port 189
3-20 Mirroring 191
3-21 Trap Event Severity 193
3-22 UpnP 195
Chapter 4: Security 196
4-1 Source Guard 196
4-1.1 Configuration 196
4-1.2 Static Table 198
4-1.3 Dynamic Table 199
4-2 ARP Inspection 200
4-2.1 Configuration 200
4-2.2 Static Table 201
4-2.3 Dynamic Table 202
4-3 DHCP Snooping 203
4-3.1 Configuration 203
4-3.2 Statistics 204
4-4 DHCP Relay 206
4-4.1 Configuration 206
4-4.2 Statistics 208
4-5 NAS 210
4-5.1 Configuration 210
4-5.2 Switch Status 219
4-5.3 Port Status 221
4-6 AAA 222
4-6.1 Configuration 222
4-6.2 Radius Overview 226
4-6.3 Radius Details 228
4-7 Port Security 233

4-7.1 Limit Control 233
4-7.2 Switch Status 236
4-7.3 Port Status 238
4-8 Access Management 239
4-8.1 Configuration 239
4-8.2 Statistics 241
4-9 SSH 242
4-10 HTTPs 243
4-11 Auth Method 244
Chapter 5: Maintenance 245
5-1 Restart 245
5-2 Firmware 246
5-2.1 Firmware Upgrade 246
5-2.2 Firmware Selection 247
5-3 Save/Restore 249
5-3.1 Factory Defaults 249
5-3.2 Save Start 250
5-3.3 Save User 251
5-3.4 Restore User 252
5-4 Export/Import 253
5-4.1 Export Config 253
5-4.2 Import Config 254
5-5 Diagnostics 255
5-5.1 Ping 255
5-5.2 Ping6 256
5-5.3 VeriPHY 257
5-6 Battery Replacement 258
Glossary of Web-Based Management 259
Contact Information 273

Introduction

Overview

This user's manual tells you how to install and connect the Vi3010 to your network system. It also explains how to configure and monitor the Vi3010 through the built-in CLI and web by (RJ-45) serial interface and Ethernet ports step-by-step. There are many detailed explanations of hardware and software functions. There are also examples of web-based interface and command-line interface (CLI) operations.

The Vi3010 series is the next generation of L2+ managed switches from Vigitron. They are affordable managed switch that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. They provides the ideal combination of affordability and capabilities for entry level networking for the small business or enterprise application and helps you create a more efficient, better-connected workforce.

Vi3010 L2+ Managed Switches provide 10 ports in a single device. The specifications are highlighted as follows:

- L2+ features provide better manageability, security, QoS, and performance.
- High port count design with all Gigabit Ethernet ports
- Support guest VLAN, voice VLAN, Port based, tag-based and Protocol based VLANs.
- Support 802.3az Energy Efficient Ethernet standard
- Support 802.3at High power PoE Plus standard
- Support IPv6/ IPv4 Dual stack
- Support s-Flow
- Support Easy-Configuration-Port for easy implement the IP Phone, IP Camera or Wireless environment.

Overview of this user's manual

- Chapter 1 "Operation of Web-based Management"
- Chapter 2 "System Configuration"
- Chapter 3 "Configuration"
- Chapter 4 "Security"
- Chapter 5 "Maintenance"

Chapter 1: Operation of Web-Based Management

Initial Configuration

This chapter instructs you how to configure and manage the Vi3010 through the web user interface. With this facility through any switch port, you can easily access and monitor the complete status of the switch, including MIBs status, port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the Vi3010 are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	

To access the Vi3010 through a network connection, type the IP address of the Vi3010 into the address box of a web browser and press "Enter". The default address of the Vi3010 is 192.168.1.1. The computer must be on the same network. If necessary, a computer can be connected directly to one of the switch ports. The computer must be setup with the same network as the Vi3010, for example, 192.168.1.100.

The default username is **"admin"** and password should be left **empty**. The first time logging in, enter the default username, and then click the **<Login>** button.

The Vi3010 supports a simple user management function to allow only one administrator to configure the system at **any one time**. *The use of simultaneous administrators could result in unpredictable operation.* **Additional** users, even with administrator's identity, **should** only monitor the system. Those who have no administrator's identity can only monitor the system. It is suggested, regardless of security level, that viewing is limited to one client at a time. Also, after accessing the Vi3010 and viewing is complete, log out.

NOTE: When you log into the switch, you must first type the admin's username and password. There is no default password so initially it should be left blank. After you type the username, please press enter. When you login Vi3010 series switch Web UI management, you can use either ipv4 or ipv6 to log into the switch.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supports neutral web browser interface.

NOTE: The Vi3010 enables DHCP, so you do not need to have a DHCP server to provide IP addresses to the switch. The switch's **default IP is 192.168.1.1.**

Connect to 192.168.20.22
The server 192.168.20.15 at Vi3010 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Figure 1: Login Page

Chapter 2: System Configuration

2-1 System Information

This chapter describes all of the basic configuration tasks, including system information and any management of the switch (e.g. Time, Account, IP, Syslog and SNMP).

2-1.1 Information

After you login, the switch shows the system information. This is the default startup page. It lists the basic information of the system, including “Model Name”, “System Description”, “Contact”, “Device Name”, “System Up Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size”, and “Flash Size”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful if the switch malfunctions.

The switch system information is provided here.

Web interface

To configure System Information in the web interface:

1. Click SYSTEM, System, Information.
2. Specify the contact information for the system administrator, the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click “Refresh”.

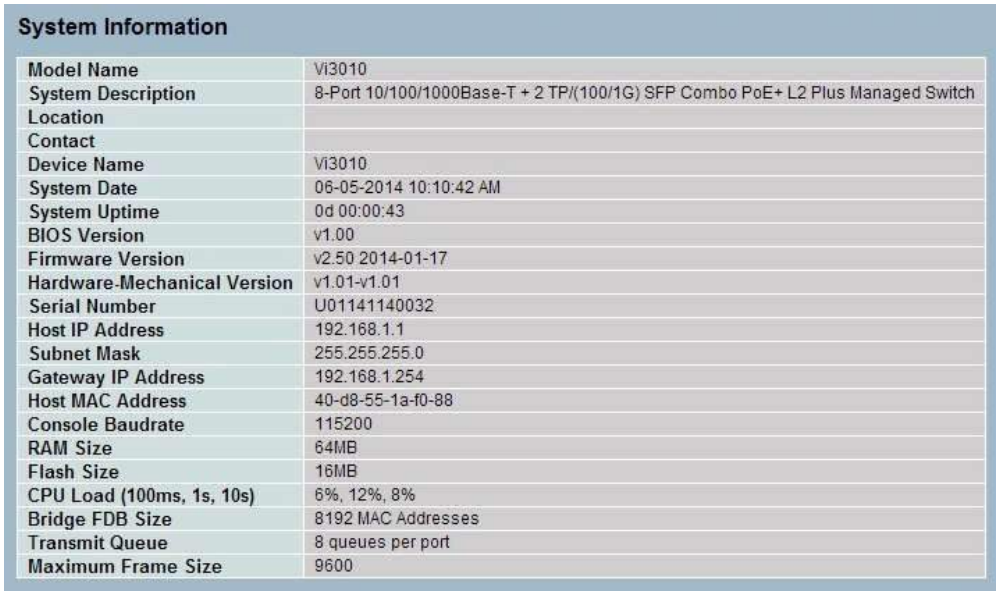

System Information
Model Name Vi3010
System Description 8-Port 10/100/1000Base-T + 2 TP/(100/1G) SFP Combo PoE+ L2 Plus Managed Switch
Location
Contact
Device Name Vi3010
System Date 06-05-2014 10:10:42 AM
System Uptime 0d 00:00:43
BIOS Version v1.00
Firmware Version v2.50 2014-01-17
Hardware-Mechanical Version v1.01-v1.01
Serial Number U01141140032
Host IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Gateway IP Address 192.168.1.254
Host MAC Address 40-d8-55-1a-f0-88
Console Baudrate 115200
RAM Size 64MB
Flash Size 16MB
CPU Load (100ms, 1s, 10s) 6%, 12%, 8%
Bridge FDB Size 8192 MAC Addresses
Transmit Queue 8 queues per port
Maximum Frame Size 9600

Figure 2-1.1: System Information

Parameter	Description
	Model name: The model name of this device.
	System description: This describes the device. This device is “8 port 10/100/1000 Base-T + 2-Port TP/(100/1G) SFP Combo PoE L2 Plus Managed Switch”.
	Location: This is the location of the switch (User-defined).
	Contact: To easily manage and maintain the device, write down the contact information of the person you would go to for help. This parameter can be configured through the device’s user interface or SNMP.
	Device name: The name of the switch (User-defined).
	System Date: This shows the system time of the switch. The format is day of week, month, day, hours: minutes: seconds, year.
	System up time: The time accumulated since this switch is powered up. The format is day, hour, minute, second.
	BIOS version: The version of the BIOS in this switch.
	Firmware version: The firmware version in this switch.
	Hardware-Mechanical version: The version of hardware and mechanical. The figure before the hyphen is the version of electronic hardware. The one after the hyphen is the version of mechanical.
	Serial number: The serial number is assigned by the manufacture.
	Host IP address: The IP address of the switch is displayed here.
	Subnet Mask: Displays the IP subnet mask assigned to the device.
	Gateway IP Address: Displays the default gateway IP address assigned to the device
	Host MAC address: This is the Ethernet MAC address of the management agent in this switch.
	Console Baud rate: Displays the baud rate of RS232 (COM) port.
	RAM size: The size of the RAM in this switch.
	Flash size: The size of the flash memory in this switch.
	CPU Load: Displays the load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals.
	Bridge FDB size: Displays the bridge FDB size information.
	Transmit Queue: Displays the device’s transmit hardware priority queue information.
	Maximum Frame size: Displays the device’s maximum frame size information.

2-1.2 Configuration

You can identify the system by configuring the contact information, name, and location of the switch.

Web interface

To configure System Information in the web interface:

1. Click System, System Information, Configuration.
2. Write System Contact , System Name, System Location information on this page.
3. Click “Apply”.

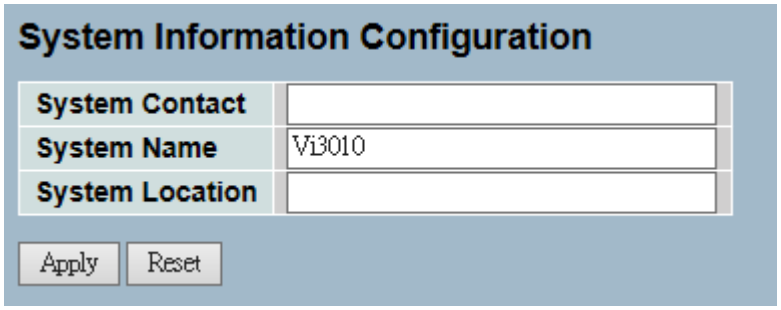


Figure 2-1.2: System Information Configuration

Parameter Description

System Contact: The textual identification of the contact person for this managed node and information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. The first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location: The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

2-2 Time

This page configure the switch's time. Time configure includes Manual Configuration and NTP Configuration.

2-2.1 Manual

The switch provides manual and automatic options to set the system time via NTP. Manual setting is simple. All you have to input is the "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item.

Web Interface

To configure Time in the web interface:

1. Click Time, Manual.
2. Specify the time parameter in manual parameters.
3. Click "Apply".

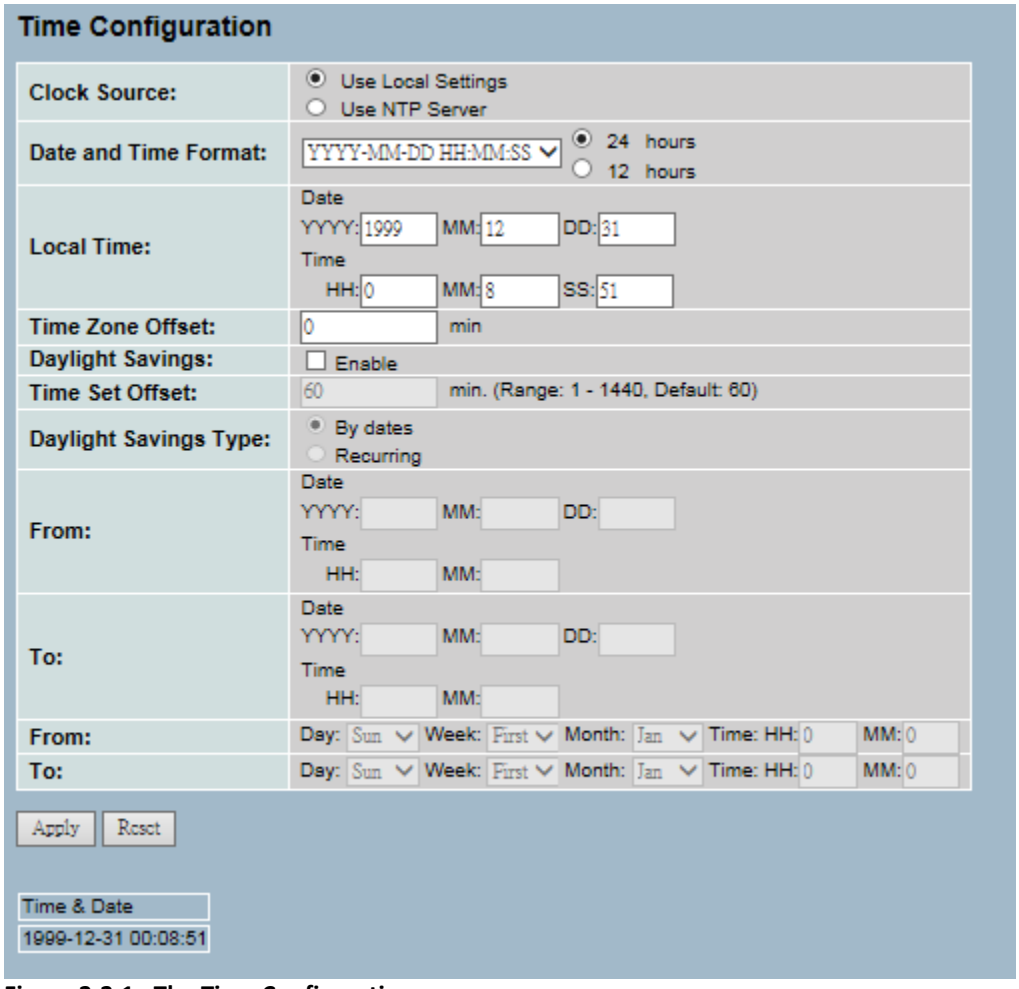


Figure 2-2.1: The Time Configuration

Parameter Description

Clock Source: Click to choose the clock source for the Vi3010. You can select "Use local Settings" or "Use NTP Server" for Vi3010 time clock source.

Date and Time Format: The drop bar is for choose appropriate time format. Three selections are provided.

YYYY-MM-DD HH:MM:SS

MM-DD-YYYY HH:MM:SS

DD-MM-YYYY HH:MM:SS

24 hours: The time is always represented in the 24-hour system.

12 hours: The time is always represented in the 12-hour system.

Local Time: Shows the current time of the system. The local time column can only be filled out or inserted in 24 hours format.

Time Zone Offset: Provides the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.

Daylight Saving: Daylight saving is adopted in some countries. If set, it will adjust the time lag or advance by the unit of hours, according to the starting date and the ending date. For example, if you set the daylight saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The valid configurable daylight saving time is –5 to +5 step one hour. A zero for this parameter means it doesn't have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date. If you set daylight saving to be non-zero, you have to set the starting/ending date as well. Otherwise, the daylight saving function will not be activated.

Time Set Offset: Provides the daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. The default is 60 minutes.

Daylight Savings Type: Provides the daylight savings type selection. You can select "By Dates" or "Recurring" two types for daylight saving type.

From: To configure the daylight saving start date and time, the format is "YYYY-MM-DD HH:MM". The column "HH: MM" can only be set up in 24 hour format.

To: To configure the daylight saving end date and time, the format is "YYYY-MM-DD HH:MM". The column "HH: MM" can only be set up in 24 hour format.

NOTE:

1. The "From" and "To" display what you set on the "From" and "To" field information.
2. The local time column and daylight saving column will not actively change by the date time format selection.

2-2.2 NTP

NTP is Network Time Protocol and is used to sync the network time based on Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server, or manually specify a user-defined NTP server and Time Zone, the switch will sync the time in a short period after pressing **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time of GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time. Otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 in 1 hour steps.

Default Time Zone: +8 Hrs.

Web Interface

To configure Time in the web interface:

1. Click SYSTEM, NTP.
2. Specify the Time parameter in manual parameters.
3. Click "Apply".

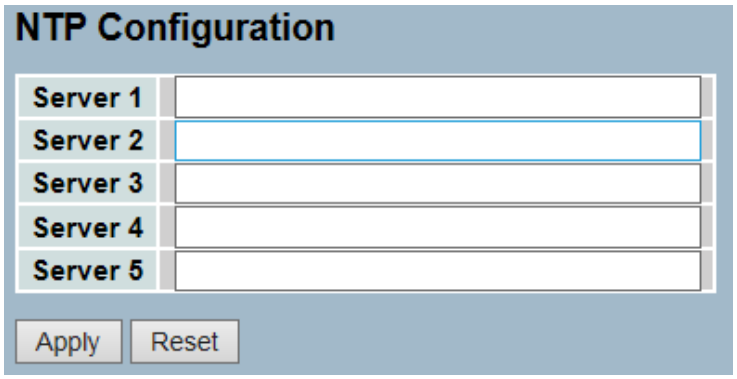


Figure 2-2.2: The NTP Configuration

Parameter Description

Server 1 to 5: Provides the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zero's. However, it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Buttons: These buttons are displayed on the NTP page:

- **Apply** – Click "Apply" to save changes.
- **Reset** – Click "Reset" to undo any changes made locally and reverts to previously saved values.

2-3 Account

In this function, only the administrator can create, modify or delete the username and password. The administrator can modify other guest identities' password without confirming the password, but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and cannot be deleted. In addition, up to 4 guest accounts can be created.

2-3.1 Users

This page provides an overview of the current users. Currently, the only way to login as another user on the web server is to close and reopen the browser.

Web Interface

To configure Account in the web interface:

1. Click SYSTEM, Account, Users.
2. Click "Add New User".
3. Specify the user name parameter.
4. Click "Apply".

Figure 2- 3.1: The Users Account Configuration

Parameter Description

User Name: The name identifying the user. This is also a link to Add/Edit User.

Password: To type the password. The allowed string length is 0 to 255 and the allowed content is the ASCII characters from 32 to 126.

Password (again): To type the password again. You must type the same password again in the field.

Privilege Level: The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups (e.g. Level 15 is granted the full control of the device. But others value need to refer to each group privilege level). User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most group privilege is level 5 and has the read-only access and privilege level 10 has the read-write access. The system maintenance (software upload, factory defaults and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

2-3.2 Privilege Level

This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC Snooping, LACP, LLDP, LLDP MED, MAC Table, MRP, MVR, MVRP Maintenance Mirroring, POE Ports, Private VLANs, QoS, SMTP, SNMP, Security, Spanning Tree, System Trap Event, VCL, VLANs, Voice VLAN, and Privilege Levels from 1 to 15.

Web Interface

To configure Privilege Level in the web interface:

1. Click SYSTEM, Account, Privilege Level.
2. Specify the privilege parameter.
3. Click “Apply”.

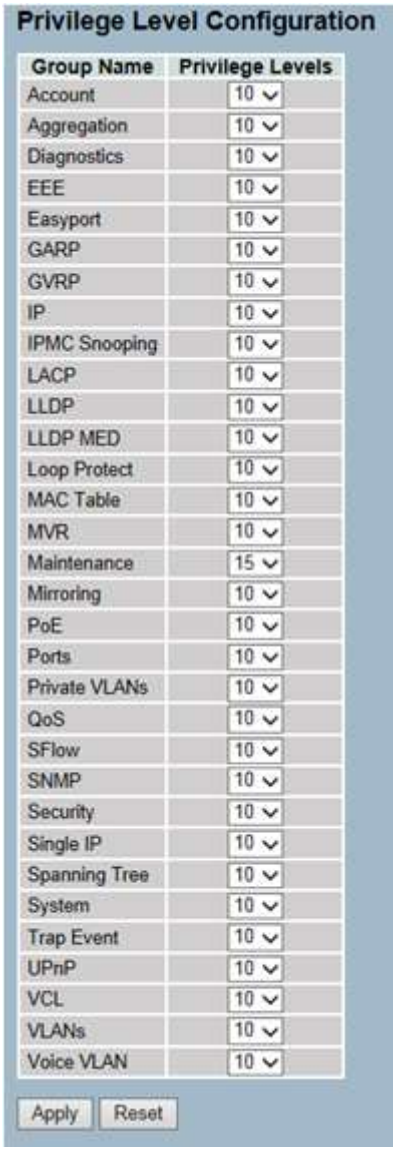


Figure 2- 3.2: The Privilege Level Configuration

Parameter Description

Group Name: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. The following description defines these privilege level groups in details:

- **System:** Contact, Name, Location, Time zone, Log.
- **Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC-based, and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, and IP source guard.
- **IP:** Everything except 'ping'.
- **Port:** Everything except 'VeriPHY'.
- **Diagnostics:** 'ping' and 'VeriPHY'.
- **Maintenance:** CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web-Users, Privilege Levels and everything in Maintenance.
- **Debug:** Only present in CLI.

Privilege Levels: Every group has an authorization privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User privilege should be same or greater than the authorization privilege level to have the access to that group.

2-4 IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

2-4.1 IPV4

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

- Configure the switch-managed IP information on this page.
- The “Configured” column is used to view or change the IP configuration.
- The “Current” column is used to show the active IP configuration.

Web Interface

To configure an IP address in the web interface:

1. Click System, IP Configuration.
2. Specify the IPv4 settings and enable DNS proxy service, if required.
3. Click “Apply”.

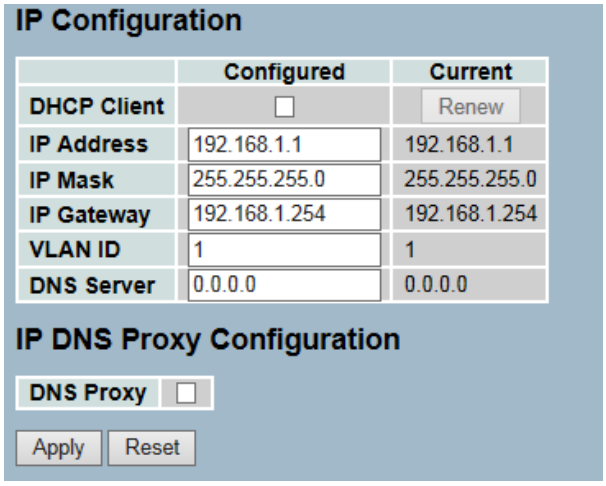


Figure 2-4.1: The IP Configuration

Parameter Description

DHCP Client: Enables the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If the DHCP fails and the configured IP address is non-zero, the DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured system name as hostname to provide DNS lookup.

IP Address: Provides the IP address of this switch in dotted decimal notation.

IP Mask: Provides the IP mask of this switch dotted decimal notation.

IP Gateway: Provides the IP address of the router in dotted decimal notation.

VLAN ID: Provides the managed VLAN ID. The allowed range is 1 to 4095.

DNS Server: Provides the IP address of the DNS Server in dotted decimal notation.

DNS Proxy: When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT and reply as a DNS resolver to the client device on the network.

2-4.2 IPV6

This section describes how to configure the switch-managed IPv6 information. The “Configured” column is used to view or change the IPv6 configuration. The “Current” column is used to show the active IPv6 configuration.

- Configure the switch-managed IPv6 information on this page.
- The “Configured” column is used to view or change the IPv6 configuration.
- The “Current” column is used to show the active IPv6 configuration.

Web Interface

To configure management IPv6 of the switch in the web interface:

1. Click System, IPv6 Configuration.
2. Specify the IPv6 settings and enable Auto Configuration service, if required.
3. Click “Apply”.

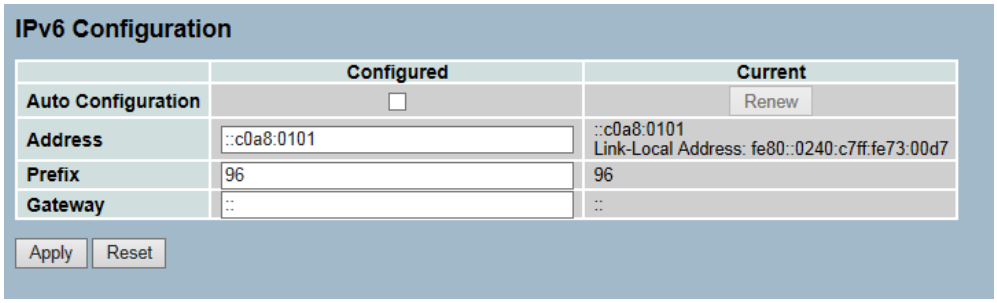


Figure 2- 4.2: The IPv6 Configuration

Parameter Description

Auto Configuration: Enables IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

Address: Provides the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zero’s. However, it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Prefix: Provides the IPv6 Prefix of this switch. The allowed range is 1 to 128.

Gateway: Provides the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zero’s. However, it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

2-5 Syslog

The syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

2-5.1 Configuration

This section describes how to configure the system log to a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure Syslog configuration in the web interface:

1. Click SYSTEM, Syslog.
2. Specify the syslog parameters, including IP Address of the syslog server and port number.
3. Evoke the sylog to enable it.
4. Click “Apply”.

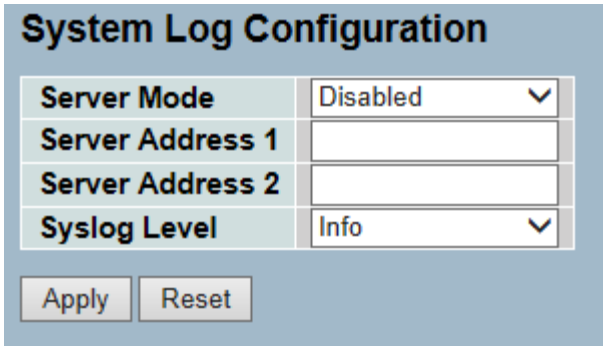


Figure 2- 5.1: The System Log Configuration

Parameter Description

Server Mode: Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. Possible modes are:

- **Enabled**: Enables server mode operation.
- **Disabled**: Disables server mode operation.

Server Address 1 and 2: Indicates the IPv4 host addresses of syslog server 1 and server 2 (for redundancy). If the switch provide DNS feature, it also can be a host name.

Syslog Level: Indicates what kind of message will send to syslog server. Possible modes are:

- **Info**: Sends information, warnings and errors.
- **Warning**: Sends warnings and errors.
- **Error**: Sends errors.

2-5.2 Log

This section describes the system log information of the switch.

Web Interface

To display the log configuration in the web interface:

1. Click Syslog, Log.
2. Display the log information.

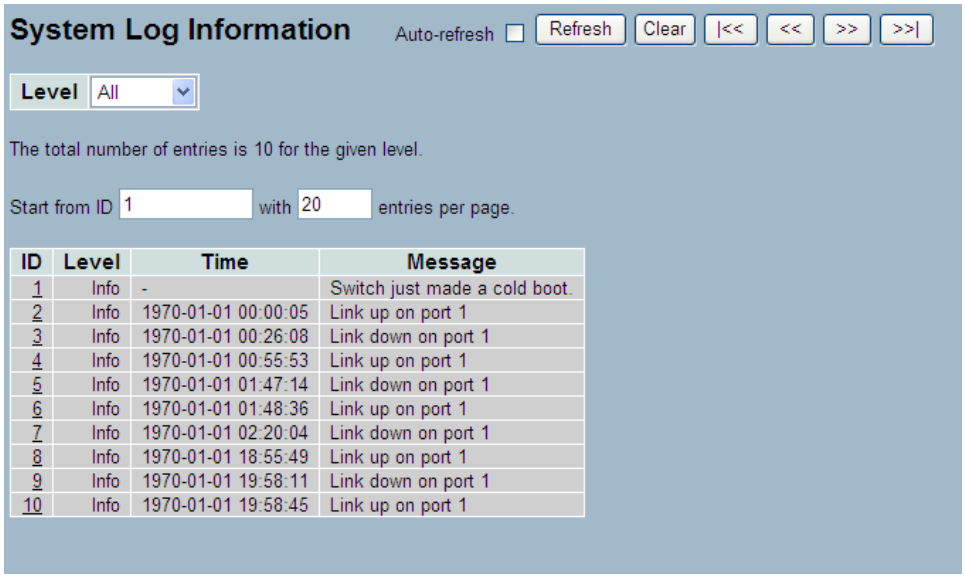

System Log Information
Auto-refresh
Refresh
Clear
|<<
<<
>>
>>|
Level
All
The total number of entries is 10 for the given level.
Start from ID 1 with 20 entries per page.
ID Level Time Message
1 Info - Switch just made a cold boot.
2 Info 1970-01-01 00:00:05 Link up on port 1
3 Info 1970-01-01 00:26:08 Link down on port 1
4 Info 1970-01-01 00:55:53 Link up on port 1
5 Info 1970-01-01 01:47:14 Link down on port 1
6 Info 1970-01-01 01:48:36 Link up on port 1
7 Info 1970-01-01 02:20:04 Link down on port 1
8 Info 1970-01-01 18:55:49 Link up on port 1
9 Info 1970-01-01 19:58:11 Link down on port 1
10 Info 1970-01-01 19:58:45 Link up on port 1

Figure 2- 5.2: The System Log Configuration

Parameter Description

Auto-refresh: To evoke the auto-refresh icon, then the device will refresh the log automatically.

Level: Level of the system log entry. The following level types are supported: Information level of the system log.

- **Warning:** Warning level of the system log.
- **Error:** Error level of the system log. All: All levels.

ID: ID (>= 1) of the system log entry.

Time: It will display the log record by device time. The time of the system log entry.

Message: It will display the log detail message. The message of the system log entry.

Upper right icon (Refresh, clear…): Click “Refresh” to refresh the system log or clear them manually. Click other buttons to move to the next or previous page.

2-5.3 Detailed Log

This section describes the detailed log information of the switch.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Syslog, Detailed Log.
2. Display the log information.

Figure 2- 5.3: The Detailed System Log Information

Parameter Description

ID: The ID (>= 1) of the system log entry.

Message: The detailed message of the system log entry.

Upper right icon (Refresh, clear…): Click “Refresh” to refresh the system log or clear them manually. Click other buttons to move to the next or previous page.

2-6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent, and traverses the object identity (OID) of the management Information base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP to “Enable”, the SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set to “Disable”, the SNMP agent will be de-activated, and the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

2-6.1 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings including community name, trap host, public traps, and the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, and then it can access the MIB information of the target device. So, both parties must have the same community name. Once the setting is complete, click **<Apply>** button so the setting can take effect.

Web Interface

To display the configure SNMP System in the web interface:

1. Click SNMP, System.
2. Evoke SNMP State to enable or disable the SNMP function.
3. Specify the “Engine ID”.
4. Click “Apply”.

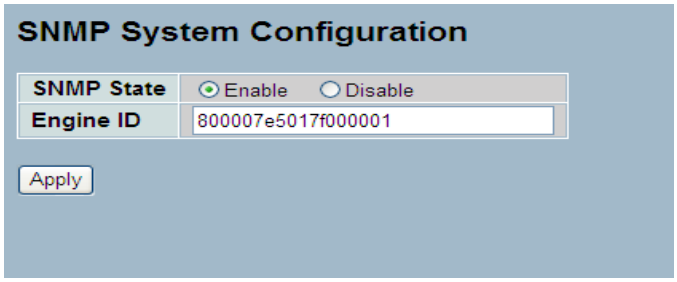


Figure 2- 6.1: The SNMP System Configuration

Parameter Description

These parameters are displayed on the SNMP System Configuration page:

SNMP State: The SNMP state is used for the activation or de-activation of SNMP.

- **Enable:** Enables SNMP state operation.
- **Disable:** Disables SNMP state operation.
- **Default:** Enable.

Engine ID: SNMPv3 engine ID. syntax: 0-9, a-f, A-F, min 5 octet, max 32 octet, fifth octet, can't input 00. If the Engine ID is changed, that will clear all original users.

2-6.2 Configuration

The function is used to configure SNMP communities. To enable a new community statistics, please check the button ▼, and choose **<Enable>** to configure SNMP function.

Web Interface

To display the SNMP Configuration in the web interface:

1. Click SNMP, Configuration.
2. Evoke “SNMP State” to enable or disable the SNMP function.
3. Click “Apply”.

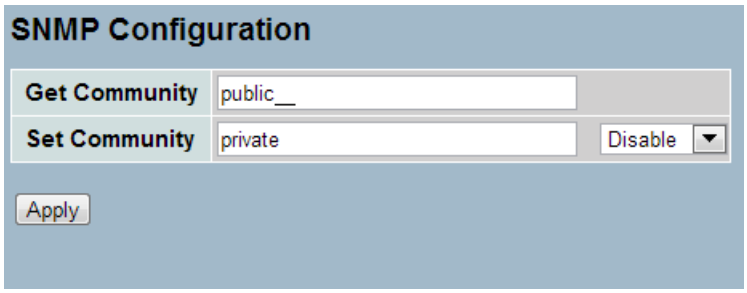


Figure2- 6.2: The SNMP Configuration

Parameter Description

These parameters are displayed on the SNMP System Configuration page:

Get Community: Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 32. The allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure the security name than a SNMPv1 or SNMPv2c community string. In addition to the community string, a particular range of source addresses can be used to restrict source subnet.

Set Community: Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure the security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Mode: Indicates the “Set Community” mode operation. Possible modes are:

- **Enabled**: Enables Set Community.
- **Disabled**: Disables Set Community.

2-6.3 Communities

The function is used to configure SNMPv3 communities. The Community and User Name are unique. To create a new community account, please check the **<Add new community>** button and enter the account information. Click **<Save>** when you're finish. Max Group Number: 4.

Web Interface

To display the configure SNMP Communities in the web interface:

1. Click SNMP, Communities.
2. Click "Add new community".
3. Specify the SNMP community's parameters.
4. Click "Apply".
5. If you want to modify or clear the setting, then click "Reset".

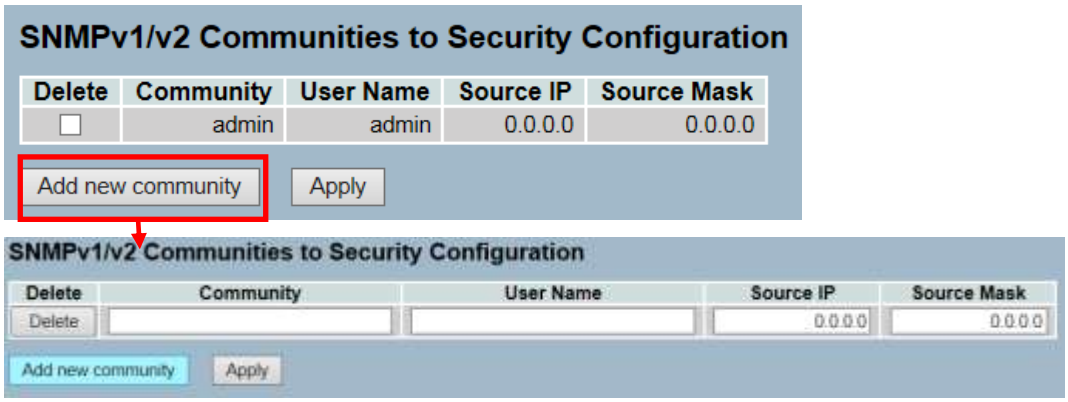


Figure 2- 6.2: The SNMPv1/v2 Communities Security Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as the security name and map a SNMPv1 or SNMPv2c community string.

User Name: The user Name access string to permit access to SNMPv3 agent. The length of "user Name" string is restricted to 1-32.

Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask: Indicates the SNMP access source address mask.

2-6.4 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new User Name account, please check the <**Add New User>** button and enter the user information. Check **<Save>** when you're finish. Max Group Number: 10.

Web Interface

To display the configure SNMP Users in the web interface:

1. Click SNMP, Users.
2. Specify the Privilege parameter.
3. Click "Apply".

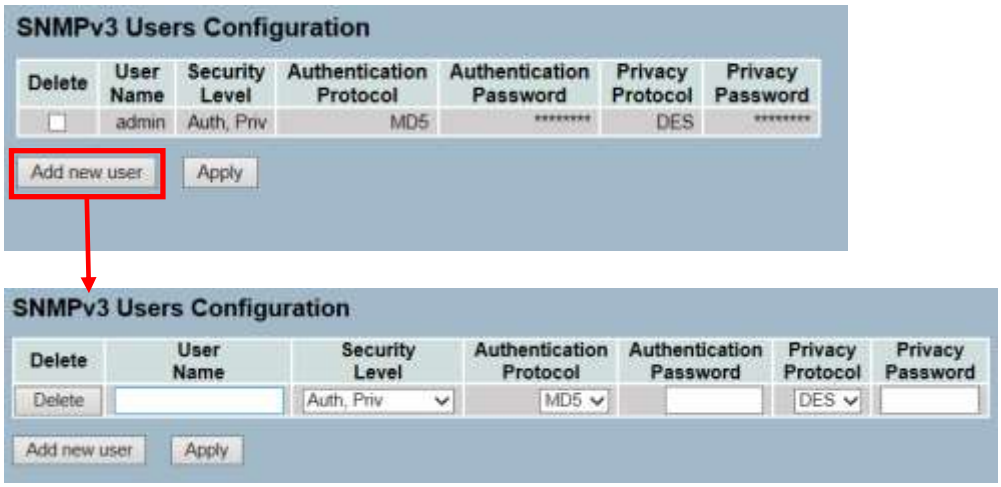


Figure 2-6.3: The SNMP Users Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: Indicates the security model that this entry should belong to. Possible security models are:

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.
- The value of security level cannot be modified if entry already exists. It must first be ensured that the value is set correctly.

Authentication Protocol: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- **MD5:** An optional flag to indicate that this user uses MD5 authentication protocol.
- **SHA:** An optional flag to indicate that this user uses SHA authentication protocol.
- The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- **DES:** An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

2-6.5 Groups

The function is used to configure SNMPv3 group. The entry index keys are Security Model and Security Name. To create a new group account, please check <**Add New Group>** button. Enter the group information, then check **<Save>.** Max Group Number: v1:2, v2:2, v3:10.

Web Interface

To display the configure SNMP Groups in the web interface:

1. Click SNMP, Groups.
2. Specify the privilege parameter.
3. Click “Apply”.

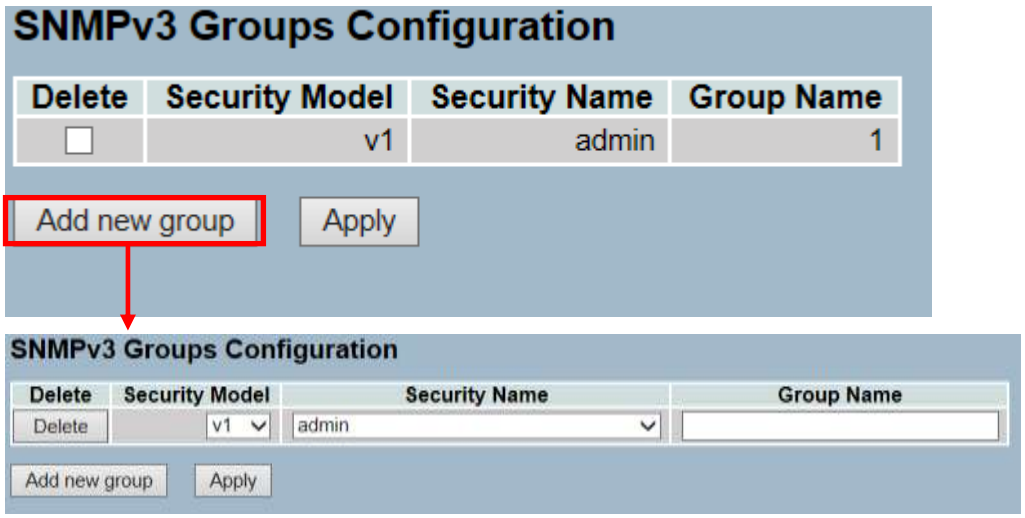


Figure 2-6.4: The SNMP Groups Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- **v1**: Reserved for SNMPv1.
- **v2c**: Reserved for SNMPv2c.
- **usm**: User-based Security Model (USM).

Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

2-6.6 Views

The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please check **<Add New View>** button. Enter the view information, then check **<Save>.** Max Group Number: 28.

Configure the SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

1. Click SNMP, Views.
2. Click “Add New View”.
3. Specify the SNMP view parameters.
4. Click “Apply”.
5. If you want to modify or clear the setting, then click “Reset”.

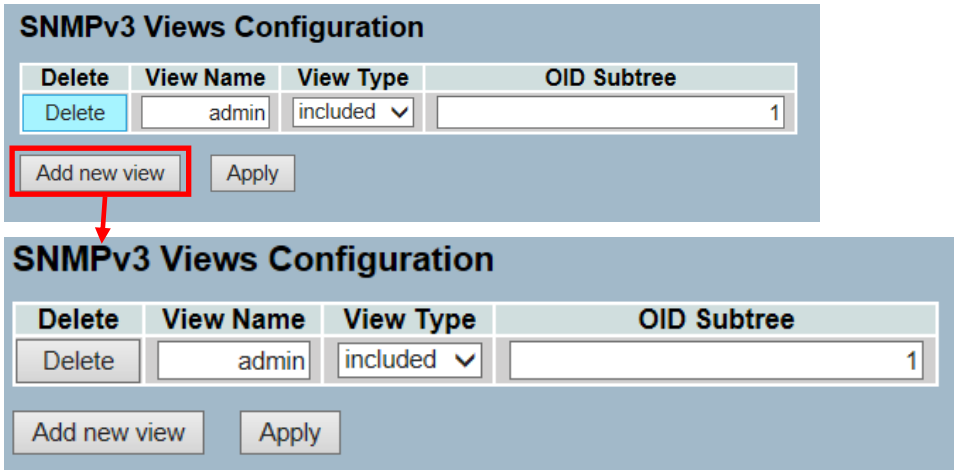


Figure 2-6.5: The SNMP Views Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type: Indicates the view type that this entry should belong to. Possible view types are:

- **Included:** An optional flag to indicate that this view subtree should be included.
- **Excluded:** An optional flag to indicate that this view subtree should be excluded.
- In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree: The OID defines the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is a digital number or asterisk (*).

Apply: Click “Save” to save the configuration to ROM.

2-6.7 Access

The function is used to configure SNMPv3 accesses. The entry index key are Group Name, Security Model, and Security level. To create a new access account, please check **<Add New Access>** button. Enter the access information, then check **<Save>**. Max Group Number: 14.

Web Interface

To display the configure SNMP Access in the web interface:

1. Click SNMP, Accesses.
2. Click “Add New Access”.
3. Specify the SNMP access parameters.
4. Click “Apply”.
5. If you want to modify or clear the setting, then click “Reset”.

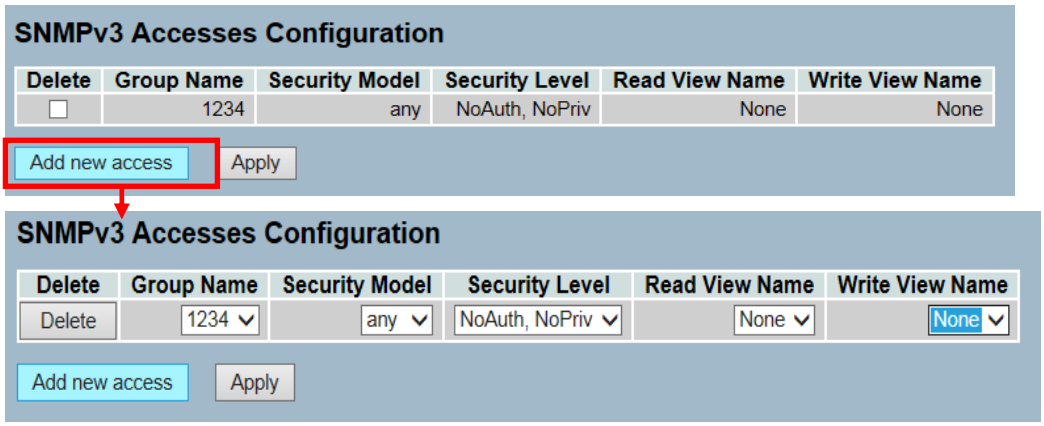


Figure 2-6.6: The SNMP Accesses Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- **Any:** Any security model accepted (v1|v2c|usm).
- **V1:** Reserved for SNMPv1.
- **V2C:** Reserved for SNMPv2c.
- **USM:** User-based Security Model (USM).

Security Level: Indicates the security model that this entry should belong to. Possible security models are:

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

Read View Name: The name of the MIB view defines the MIB objects so it may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. Write view name.

The name of the MIB view defines the MIB objects so this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name: The name of the MIB view defines the MIB objects so this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Button:

- **Add new access -** Click to add a new access entry.
- **Apply -** Click “Apply” to apply changes.

2-6.8 Trap

The function is used to configure SNMP trap. To create a new trap account, please check **<No number>** button. Enter the trap information, then check **<Apply>**. Max Group Number: 6.

Web Interface

To configure SNMP Trap setting:

1. Click SNMP, Trap.
2. Display the SNMP trap hosts information table.
3. Choose an entry to display and modify the detail parameters, or click the delete button to delete the trap hosts entry.

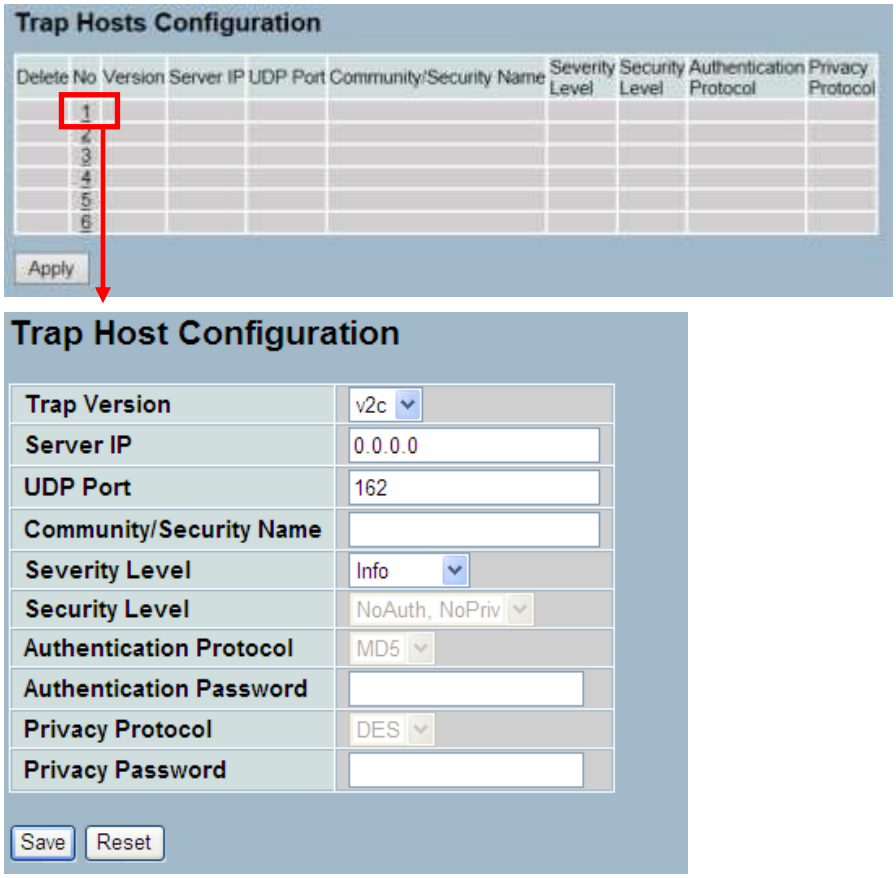


Figure 2-6.7: The SNMP Trap Host Configuration

Parameter Description

Delete: Check **<Delete>** entry, then check **<Save>** button to delete the entry.

Trap Version: You may choose V2C or V3 trap.

Server IP: To assign the SNMP Host IP address.

UDP Port: To assign a port number. The default is 162.

Community / Security Name: The length of "Community / Security Name" string is restricted to 1-32.

Security Level: Indicates what kind of message will send to security level. Possible modes are:

- **Error:** Send errors.
- **Warning:** Send warnings and errors.
- **Info:** Send information, warnings, and errors.

Security Level: There are three kinds of choices.

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

Authentication Protocol: You can choose MD5 or SHA for authentication.

Authentication Password: The length of 'MD5 Authentication Password' is restricted to 8 – 32. The length of 'SHA Authentication Password' is restricted to 8 – 40.

Privacy Protocol: You can set DES encryption for User Name.

Privacy Password: The length of ' Privacy Password ' is restricted to 8 – 32.

Chapter 3: Configuration

This chapter describes the basic network configuration tasks which includes the Ports, Layer 2 network protocol (e.g. VLANs, QoS, IGMP, ACLs, PoE, and so on), and any settings of the switch.

3-1 Port

The section describes to configure the port detail parameters of the switch. You could also use the port configuration to enable or disable the port of the switch. Monitor the ports content or status in the function.

3-1.1 Configuration

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including:

- Linkup/Linkdown
- Speed (Current and Configured)
- Flow Control (Current Rx, Current Tx, and Configured)
- Maximum Frame Size
- Excessive Collision Mode
- Power Control

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Configuration, Port, and then Configuration.
2. Specify the Speed Configured, Flow Control , Maximum Frame size, Excessive Collision mode, and Power Control.
3. Click “Apply”.

NOTE: The flow control will be enabled only when the PD supports flow control function.

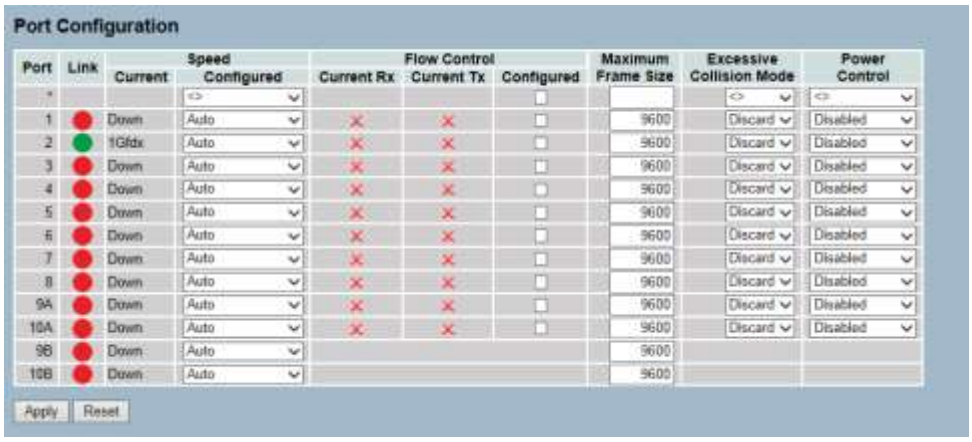


Figure 3-1.1: The Port Configuration

Parameter Description

Port: This is the logical port number for this row.

Link: The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed: Provides the current link speed of the port.

Configured Link Speed: Selects any available link speed for the given switch port.

- "Auto Speed" selects the highest speed that is compatible with a link partner.
- "Disabled" turns off the switch port operation.

Flow Control: When "Auto Speed" is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The "Current Rx" column indicates whether the pause frames on the port are obeyed, and the "Current Tx" column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last "Auto-Negotiation".

Check the configured column to use flow control. This setting is related to the setting for configured link speed.

Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode: Configure port transmit collision behavior.

- **Discard:** Discards frame after 16 collisions (default).
- **Restart:** Restarts backoff algorithm after 16 collisions.

Power Control: The usage column shows the current percentage of the power consumption per port. The configured column allows for changing the power savings mode parameters per port.

- **Disabled:** All power savings mechanisms disabled.
- **ActiPHY:** Link down power savings enabled.
- **PerfectReach:** Link up power savings enabled.
- **Enabled:** Both link up and link down power savings enabled.

3-1.2 Port Description

The section configures the port's alias or any descriptions for the port identity. It allows the user to write down an alphanumeric string to describe the full name and version identification for the system's hardware type, software version, and networking application.

Web Interface

To configure a port description in the web interface:

1. Click Configuration, Port, and then Port Description.
2. Specify the detailed port alias or description - an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click "Apply".

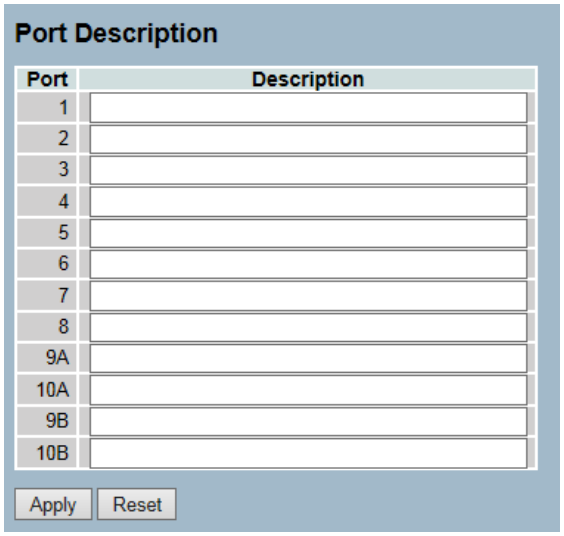


Figure 3-1.2: The Port Configuration

Parameter Description

Port: This is the logical port number for this row.

Description: Description of the device ports cannot include the following: " # % & ' + \.

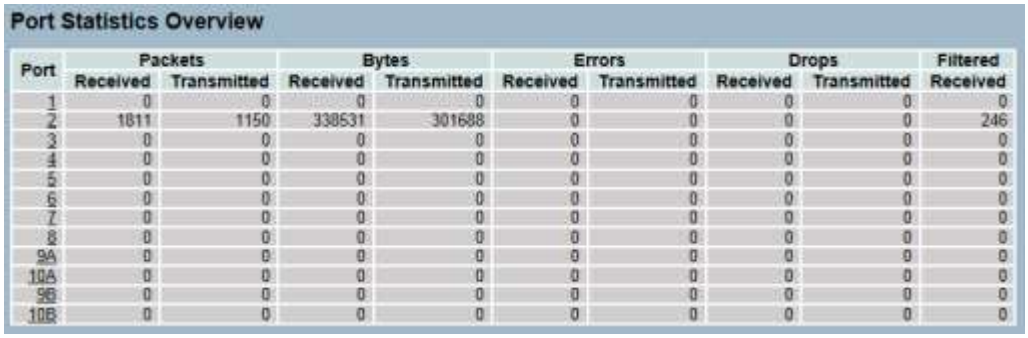
3-1.3 Traffic Overview

The section describes to the port statistics information and provides an overview of the general traffic statistics for all switch ports. The ports belong to the current selected stack unit, as reflected by the page header.

Web Interface

To display the Port Statistics Overview in the web interface:

1. Click Configuration, Port, and then Traffic Overview.
2. If you want to auto-refresh, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh“ to refresh the port statistics or clear all information by pressing “Clear”.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	1811	1150	338531	301688	0	0	0	0	246
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9A	0	0	0	0	0	0	0	0	0
10A	0	0	0	0	0	0	0	0	0
9B	0	0	0	0	0	0	0	0	0
10B	0	0	0	0	0	0	0	0	0

Figure 3-1.3: The Port Statistics Overview

Parameter Description

Port: The logical port for the settings contained in the same row.

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

Drops: The number of frames discarded due to ingress or egress congestion.

Filtered: The number of received frames filtered by the forwarding.

3-1.4 Detailed Statistics

The section provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belongs to the current selected stack unit, as reflected by the page header.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

To display the Per Port Detailed Statistics Overview in the web interface:

1. Click Configuration, Port, then Detailed Statistics.
2. Scroll the port index to select which port you want to show the detailed port statistic overview.
3. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
4. Click “Refresh“ to refresh the port detailed statistics or clear all information by pressing “Clear”.

Figure 3-1.4: The Port Detail Statistics Overview

Parameter Description

Auto-refresh: Evoke to refresh the port statistics information automatically.

Upper left scroll bar: To scroll which port to display the port statistics with “Port-0”, “Port-1...

Receive Total and Transmit Total

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode to include a PAUSE operation.

Receive and Transmit Size Counters: The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters: The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short 1 frames received with valid CRC.

Rx Oversize: The number of long 2 frames received with valid CRC.

Rx Fragments: The number of short 1 frames received with invalid CRC.

Rx Jabber: The number of long 2 frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

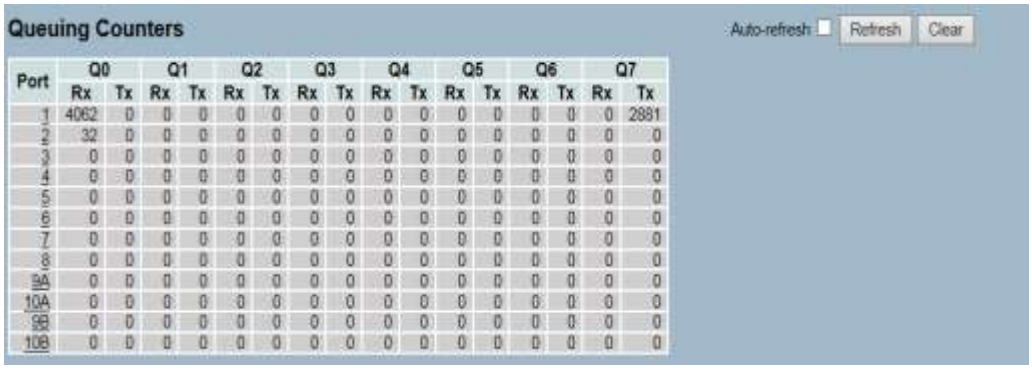
3-1.5 QoS Statistics

The section describes how the switch could display the QoS detailed queuing counters for a specific switch port. The ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the Queuing Counters in the web interface:

1. Click Configuration, Port, and then QoS Statistics.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Click "Refresh" to refresh the queuing counters or clear all information by pressing "Clear".



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	4062	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2881
2	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 3-1.5: The Queuing Counters Overview

Parameter Description

Port: The logical port for the settings contained in the same row.

Qn: Qn is the QoS queue number per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

Auto-refresh: To evoke the auto-refresh to refresh the queuing counters automatically.

Upper right icon (Refresh, clear): Click "Refresh" to refresh the queuing counters or clear them manually.

3-1.6 SFP Information

The section describes how the switch could display the detailed information of the SFP module. The information includes: Connector type, Fiber type, Wavelength, Baud Rate, Vendor OUI, and more.

Web Interface

To display the SFP information in the web interface:

1. Click Configuration, Port, and then SFP Information.
2. To display the SFP Information.

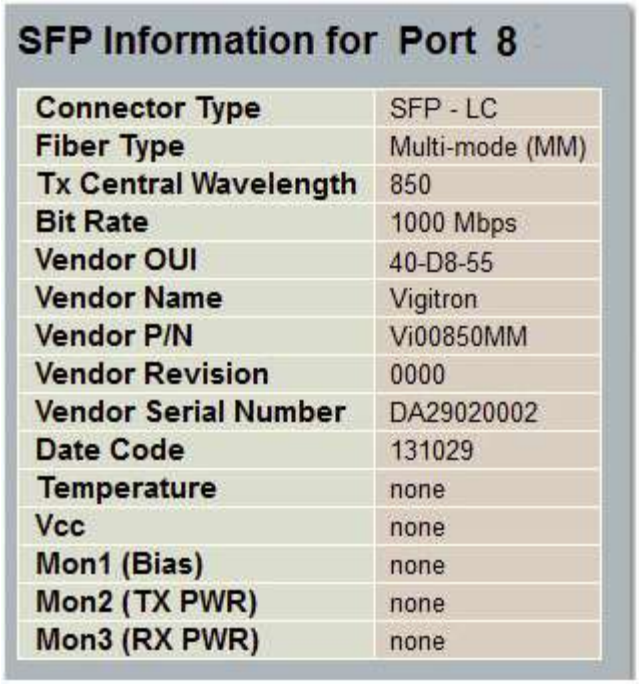


Figure 3-1.6: The SFP Information Overview

Parameter Description

Connector Type: Displays the connector type (e.g. UTP, SC, ST, LC and so on).

Fiber Type: Displays the fiber mode (e.g. Multi-Mode or Single-Mode).

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength (e.g. 850nm, 1310nm, 1550nm, and so on).

Baud Rate: Displays the maximum baud rate of the fiber module supported (e.g. 10M, 100M, 1G, and so on).

Vendor OUI: Displays the manufacturer's OUI code, which is assigned by IEEE.

Vendor Name: Displays the company name of the module manufacturer.

Vendor P/N: Displays the product name of the naming by module manufacturer.

Vendor Revision: Displays the module revision.

Vendor Serial Number: Shows the serial number assigned by the manufacturer.

Date Code: Shows the date this SFP module was made.

Temperature: Shows the current temperature of SFP module.

Vcc: Shows the working DC voltage of SFP module.

Mon1(Bias) mA: Shows the Bias current of SFP module.

Mon2(TX PWR): Shows the transmit power of SFP module.

Mon3(RX PWR): Shows the receiver power of SFP module.

NOTE: Only SFP modules that are UL and CDRH Certified and have an international certification such as TUV, VDE, or DEMKO are recommended. Use only Class 1 SFP modules.

3-1.7 EEE

The section allows the user to inspect and configure the current EEE port settings.

EEE is a power saving option that reduces power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting devices have all circuits powered up when traffic is transmitted. The devices can exchange information about the wakeup time using the LLDP protocol.

To maximize power saving, the circuit doesn't start once the transmit data is ready for a port. Instead, it's queued until 3000 bytes of data are ready to be transmitted. To avoid a large delay in case there is data less than 3000 bytes waiting to be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

If desired, it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue through QOS, and then mark the queue as an urgent queue. When an urgent queue gets data ready to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Web Interface

To configure the EEE Configuration in the web interface:

1. Click Configuration, Port, and then EEE.
2. To evoke which port you want to enable the EEE function.
3. To evoke which "EEE Urgent Queues" level, ranging from 1 to 8. The queue will postpone the transmission until 3000 bytes of data are ready to be transmitted.
4. Click "Save" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

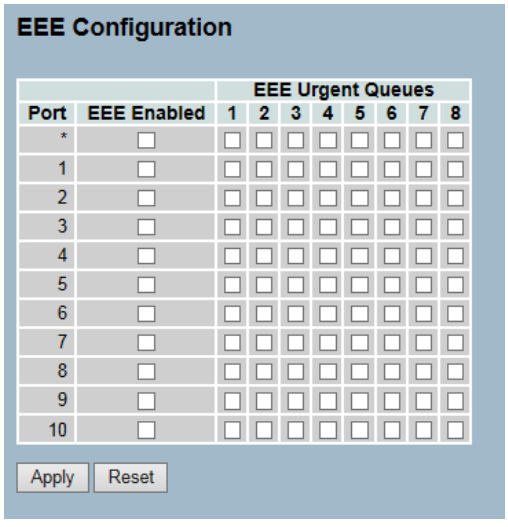


Figure 3-1.7: The EEE Configuration

Parameter Description

EEE Port Configuration: The EEE port settings relate to the currently selected stack unit, as reflected by the page header.

Port: The switch port number of the logical EEE port.

EEE Enabled: Controls whether EEE is enabled for this switch port.

EEE Urgent Queues: Queues set will activate transmission of frames as soon as any data is available. Otherwise, the queue will postpone the transmission until 3000 bytes of data are ready to be transmitted.

3-2 ACL

The Vi3010 switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering. It also selects the types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes - IPv4, ARP protocol, MAC, and VLAN parameters. This section will go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port. The policy number is 1-8. However, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

3-2.1 Ports

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port, unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, ACL, and then Ports.
2. Scroll the specific parameter value to select the correct value for port ACL setting.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.
5. After the configuration is complete, then you could see the counter of the port. You could click refresh to update the counter or clear the information.

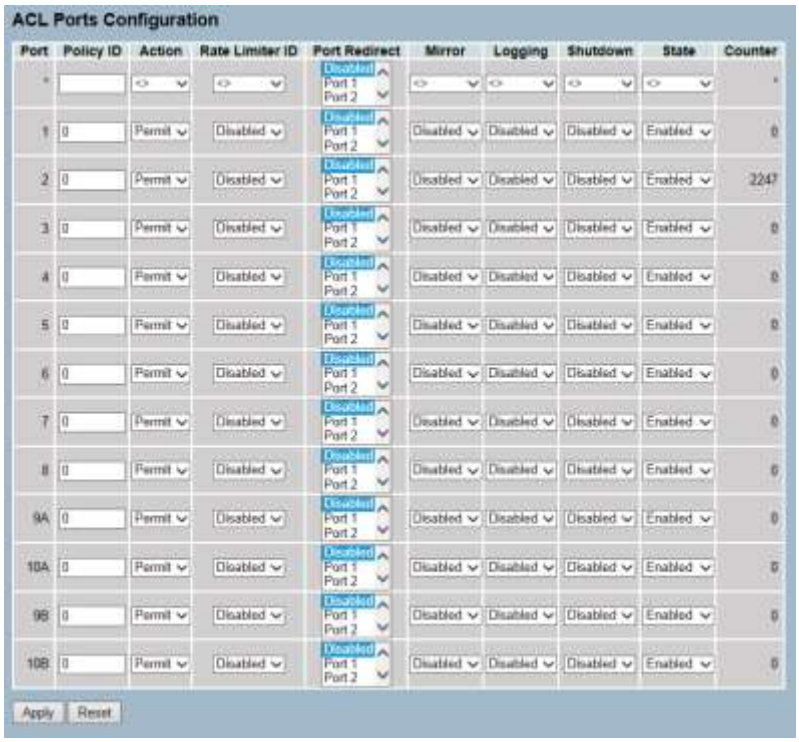


Figure 3-2.1: The ACL Ports Configuration

Parameter Description

Port: The logical port for the settings contained in the same row.

Policy ID: Selects the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action: Selects whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID: Selects which rate limiter to apply on this port. The allowed values are “Disabled” or the values from 1 through 16. The default value is "Disabled".

Port Redirect: Selects which port frames are redirected on. The allowed values are “Disabled” or a specific port number. The default value is "Disabled".

Mirror: Specifies the mirror operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

Logging: Specifies the logging operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are stored in the system log.
- **Disabled:** Frames received on the port are not logged.
- The default value is "Disabled". Please note that the system log memory size and logging rate is limited.

Shutdown: Specifies the port shut down operation of this port. The allowed values are:

- **Enabled:** If a frame is received on the port, the port will be disabled.
- **Disabled:** The port shut down is disabled.
- The default value is "Disabled".

State: Specifies the port state of this port. The allowed values are:

- **Enabled:** To reopen ports, change the volatile port configuration of the ACL user module.
- **Disabled:** To close ports, change the volatile port configuration of the ACL user module.
- The default value is "Enabled".

Counter: Counts the number of frames that match this ACE.

Buttons

- **Apply** – Click to apply changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh, clear): Click “Refresh” to refresh the ACL Port Configuration or clear them manually.

3-2.2 Rate Limiters

The section describes how to configure the switch's ACL rate limiter parameters. The "Rate Limiter Level" from 1 to 16 allows the user to set the rate limiter value and units with pps or kbps.

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, ACL, and then Rate Limiter.
2. Specify the "Rate" field. The range is from 0 to 3276700.
3. Scroll the "Unit" to pps or kbps.
4. Click "Save" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

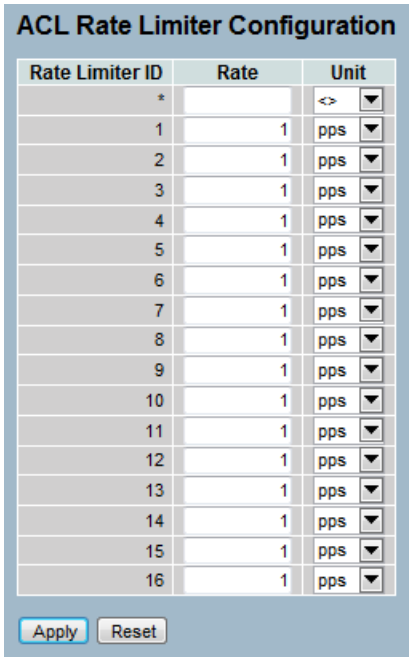


Figure 3-2.2: The ACL Rate Limiter Configuration

Parameter Description

Rate Limiter ID: The rate limiter ID for the settings contained in the same row.

Rate: The allowed values are: "0-3276700" in pps or "0, 100, 200, 300... 1000000" in kbps.

Unit: Specifies the rate unit. The allowed values are:

- **Pps:** Packets per second
- **Kbps:** Kbits per second

Buttons

- **Apply** – Click to apply changes.
- **Reset** - Click "Reset" to undo any changes made locally and revert to previously saved values.

3-2.3 Access Control List

The section describes how to configure the Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs, used for internal protocol, cannot be edited or deleted. The order sequence cannot be changed and the priority is highest.

Web Interface

To configure Access Control List in the web interface:

1. Click Configuration, ACL, and then Access Control List.
2. Click the ⊕ button to add a new ACL, or use the other ACL modification buttons to specify the editing action (e.g. edit, delete, or moving the relative position of entry in the list).
3. Specifies the parameter of the ACE.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the items displayed depends on various selections, such as frame type and IP protocol type. Specifies the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as rate limiter, port copy, logging, or shutdown).

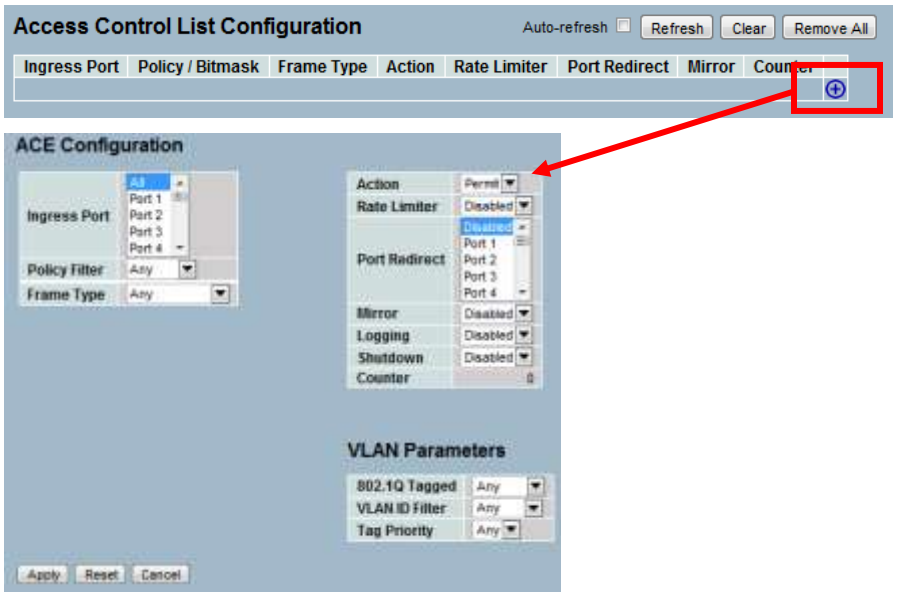


Figure 3-2.3: The ACL Rate Limiter Configuration

Parameter Description

Ingress Port: Selects the ingress port for which this ACE applies.

- **All:** The ACE applies to all port.
- **Port n:** The ACE applies to this port number, where “n” is the number of the switch port.

Policy Filter: Specifies the policy number filter for this ACE.

- **Any:** No policy filter is specified (the policy filter status is "don't-care").
- **Specific:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears.

Frame Type: Indicates the frame type of the ACE. Possible values are:

- **Any:** The ACE will match any frame type.
- **Ethernet Type:** Only Ethernet type frames can match this ACE. The IEEE 802.3 describes the value of “Length/Type Field” specifications to be greater than or equal to 1536 decimal (equals to 0600 hexadecimal).
- **ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.
- **IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.

Action: Specifies the action to take with a frame that hits this ACE.

- **Permit:** The frame that hits this ACE is granted permission for the ACE operation.
- **Deny:** The frame that hits this ACE is dropped.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When “Disabled” is displayed, the rate limiter operation is disabled.

Port Redirect: Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. “Disabled” indicates that the port redirect operation is disabled.

Mirror: Specifies the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

Logging: Indicates the logging operation of the ACE. Possible values are:

- **Enabled:** Frames matching the ACE are stored in the system log.
- **Disabled:** Frames matching the ACE are not logged.
- Please note that the system log memory size and logging rate is limited.

Shutdown: Indicates the port shut down operation of the ACE. Possible values are:

- **Enabled:** If a frame matches the ACE, the ingress port will be disabled.
- **Disabled:** Port shut down is disabled for the ACE.

Counter: The counter indicates the number of times the ACE was hit by a frame.

VLAN Parameters

802.1Q Tagged: Specifies whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

- **Any:** Any value is allowed ("don't-care").
- **Enabled:** Tagged frame only.
- **Disabled:** Untagged frame only.
- The default value is "Any".

VLAN ID Filter: Specifies the VLAN ID filter for this ACE.

- **Any:** No VLAN ID filter is specified (VLAN ID filter status is "don't-care").
- **Specific:** If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID: When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4094. A frame that hits this ACE matches this VLAN ID value.

Tag Priority: Specifies the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value “Any” means that no tag priority is specified (tag priority is "don't-care").

Modification Buttons: You can modify each ACE (Access Control Entry) in the table using the following buttons:

: Inserts a new ACE before the current row.

: Edits the ACE row.

: Moves the ACE up the list.

: Moves the ACE down the list.

: Deletes the ACE.

: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons:

- **Apply** – Click to apply changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert to previously saved values.

Auto-refresh: To evoke the auto-refresh to refresh the information automatically.

Upper right icon (Refresh, Clear, Remove All): Click “Refresh” to refresh the ACL configuration or clear them manually. You can also remove or clean up all ACL configurations in the table.

3-2.4 ACL Status

The section shows the ACL status by different ACL users. Each row describes the ACE defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Configuration, ACL, and then ACL status.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Click "Refresh" to refresh the ACL Status.

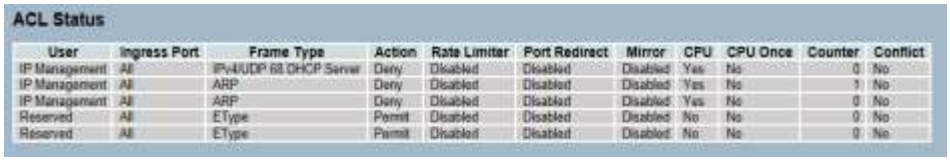

ACL Status
User Ingress Port Frame Type Action Rate Limiter Port Redirect Mirror CPU CPU Once Counter Conflict
IP Management All IPv4/UDP 68 DHCP Server Deny Disabled Disabled Disabled Yes No 0 No
IP Management All ARP Deny Disabled Disabled Disabled Yes No 1 No
IP Management All ARP Deny Disabled Disabled Disabled Yes No 0 No
Reserved All EType Permit Disabled Disabled Disabled No No 0 No
Reserved All EType Permit Disabled Disabled Disabled No No 0 No

Figure 3-2.4: The ACL Rate Limiter Configuration

Parameter Description

User: Indicates the ACL user.

Ingress Port: Indicates the ingress port of the ACE. Possible values are:

- **All:** The ACE will match all ingress port.
- **Port:** The ACE will match a specific ingress port.

Frame Type: Indicates the frame type of the ACE. Possible values are:

- **Any:** The ACE will match any frame type.
- **EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
- **ARP:** The ACE will match ARP/RARP frames.
- **IPv4:** The ACE will match all IPv4 frames.
- **IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol.
- **IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.
- **IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol.
- **IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
  IPv6: The ACE will match all IPv6 standard frames.

Action: Indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When "Disabled" is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are "Disabled" or a specific port number. When "Disabled" is displayed, the port redirect operation is disabled.

Mirror: Specifies the mirror operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are mirrored.
- **Disabled:** Frames received on the port are not mirrored.
- The default value is "Disabled".

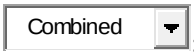
CPU: Forward packet that matched the specific ACE to CPU.

CPU Once: Forward first packet that matched the specific ACE to CPU.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Auto-refresh: To evoke the auto-refresh to refresh the information automatically.



: Select the ACL status from this drop down list.

Upper right icon (Refresh): Click “Refresh” to refresh the ACL status information manually.

3-3 Aggregation

The aggregation is used to configure the settings of “Link Aggregation”. You can bundle more than one port with the same speed, full duplex, and the same MAC to be a single logical port. Thus, the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation. For example, if there are three fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single fast Ethernet port has.

3-3.1 Static Trunk

The aggregation configuration is used to configure the settings of link aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port. Thus, the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation.

3-3.1.1 Static Trunk

Ports using static trunk as their trunk method can choose their unique static Group ID to form a logic “trunked port”. The benefit of using “Static Trunk” method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using static trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

1. Click Configuration, Aggregation, then Static Trunk.
2. Evoke to enable or disable the aggregation Hash mode function. Evoke “Aggregation Group ID” and port members.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

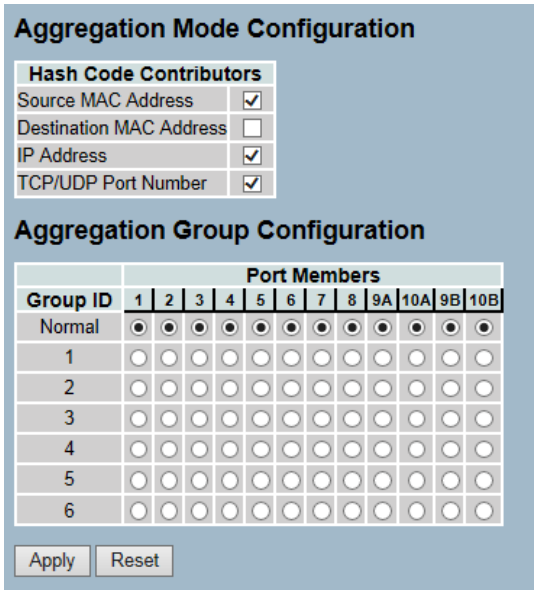


Figure 3-3.1.1: The Aggregation Mode Configuration

Parameter Description

Hash Code Contributors

Source MAC Address: The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the source MAC address or uncheck to disable. By default, the source MAC address is enabled.

Destination MAC Address: The destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the destination MAC Address or uncheck to disable. By default, the destination MAC Address is disabled.

IP Address: The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP address or uncheck to disable. By default, the IP Address is enabled.

TCP/UDP Port Number: The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP port number or uncheck to disable. By default, the TCP/UDP port number is enabled.

Aggregation Group Configuration

Group ID: Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members: Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

3-3.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP Group ID to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

3-3.2.1 Configuration

This page allows the user to inspect and change the current LACP port configurations. A LACP trunk group with more than one ready member-ports is a “Real Trunked” group. A LACP trunk group with only one or less than one ready member-ports is not a “Real Trunked” group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, Configuration.
2. Evoke to enable or disable the LACP on the port of the switch. Scroll the Key parameter with Auto or Specific. The default is “Auto”.
3. Scroll the role with “Active” or “Passive”. The default is “Active”.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, then you need to click the reset button. It will revert to previously saved values.

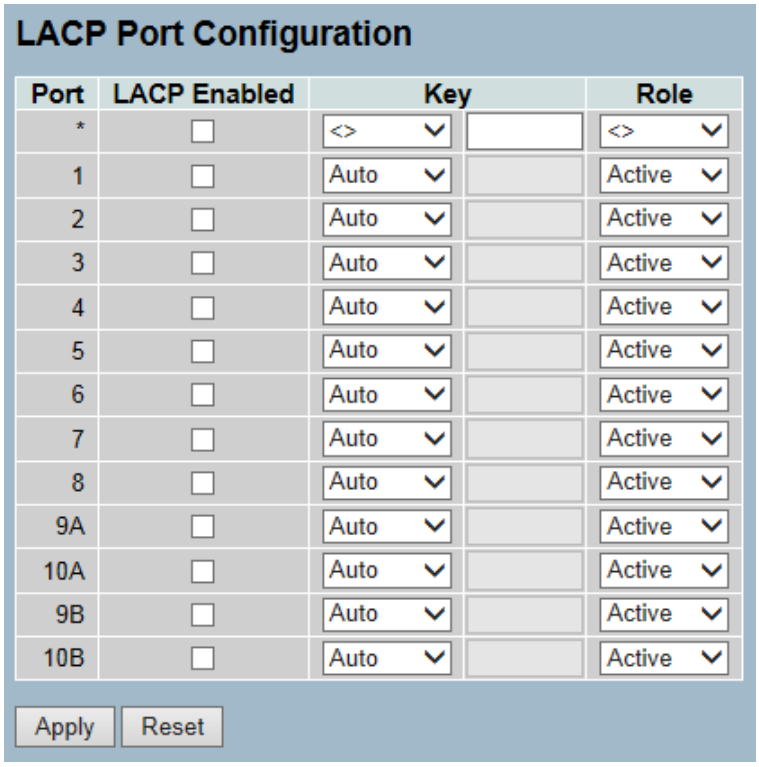


Figure 3-3.2.1: The LACP Port Configuration

Parameter Description

Port: The switch port number.

LACP Enabled: Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form a max of 12 LLAGs per switch and 2 GLAGs per stack.

Key: The key value incurred by the port, ranging from 1 to 65535. The auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1 GB = 3. By using the “Specific” setting, a user-defined value can be entered. Ports with the same key value can participate in the same aggregation group, while ports with different keys cannot.

Role: The “Role” shows the LACP activity status. The “Active” will transmit LACP packets each second; while “Passive” will wait for a LACP packet from a partner (speak if spoken to).

3-3.2.2 System Status

This section describes how the status overview for all LACP instances is provided when you complete setting the LACP function on the switch.

Web Interface

To display the LACP System status in the web interface:

1. Click Configuration, LACP, System Status.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh“ to refresh the LACP System Status.

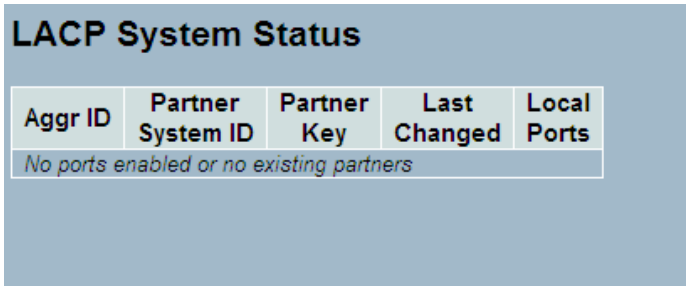


Figure 3-3.2.2: The LACP System Status

Parameter Description

Aggr ID: The aggregation ID associated with this aggregation instance. For LLAG, the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'.

Partner System ID: The system ID (MAC address) of the aggregation partner.

Partner Key: The key that the partner has assigned to this aggregation ID.

Last changed: The time since this aggregation changed.

Local Ports: Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".

3-3.2.3 Port Status

This section describes how the port status overview for all LACP instances is provided when you complete setting the LACP function on the switch.

Web Interface

To display the LACP Port status in the web interface:

1. Click Configuration, LACP, Port Status.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh“ to refresh the LACP Port Status.

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9A	No	-	-	-	-
10A	No	-	-	-	-
9B	No	-	-	-	-
10B	No	-	-	-	-

Figure 3-3.2.3: The LACP Status

Parameter Description

Port: The switch port number.

LACP: 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile, the LACP status is disabled.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID: The aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs, while IDs 3-14 are LLAGs.

Partner System ID: The partner's system ID (MAC address).

Partner Port: The partner's port number connected to this port.

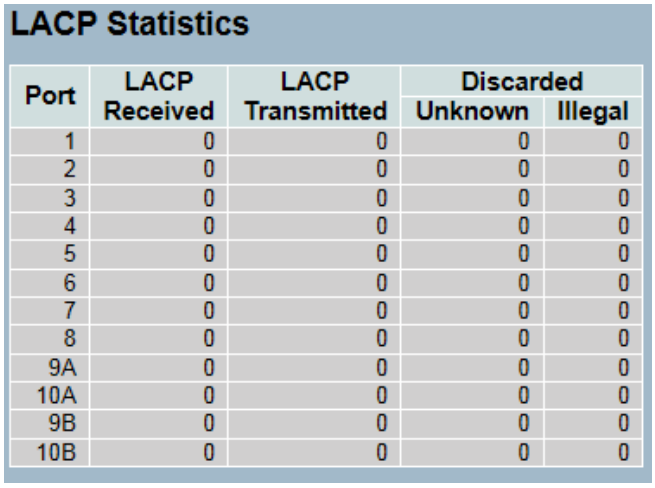
3-3.2.4 Port Statistics

This section describes how the port statistics overview is provided when you complete setting the LACP function on the switch.

Web Interface

To display the LACP Port Status in the web interface:

1. Click Configuration, LACP, Port Statistics.
2. If you want to auto-refresh the information, then you need to evoke the "Auto refresh".
3. Click "Refresh" to refresh the LACP Statistics.



LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9A	0	0	0	0
10A	0	0	0	0
9B	0	0	0	0
10B	0	0	0	0

Figure 3-3.2.4: The LACP Statistics

Parameter Description

Port: The switch port number.

LACP Received: Shows how many LACP frames have been received at each port.

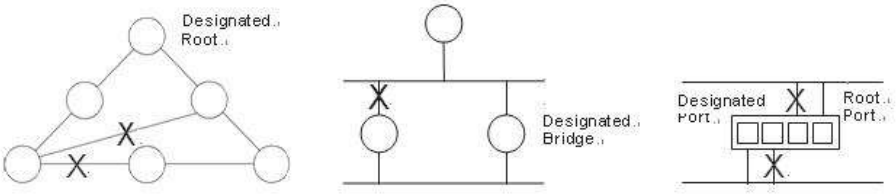
LACP Transmitted: Shows how many LACP frames have been sent from each port.

Discarded: Shows how many unknown or illegal LACP frames have been discarded at each port.

3-4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (e.g. an STP-compliant switch, bridge, or router) in your network to ensure that only one route exists between any two stations on the network. It also provides backup links, which automatically take over when the primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge, or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device), which incurs the lowest path cost when forwarding a packet from that device to the root device. Then, it selects a designated bridging device from each LAN, which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to the designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Therefore, the network packets are only forwarded between root ports and designated ports to eliminate any possible network loops.



Once a stable network topology had been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3-4.1 Bride Settings

The section describes how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings used by all STP Bridge instance in the Switch Stack.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings.
3. Evoke to enable or disable the parameters and write down available value of parameters in blank field in Advanced settings.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

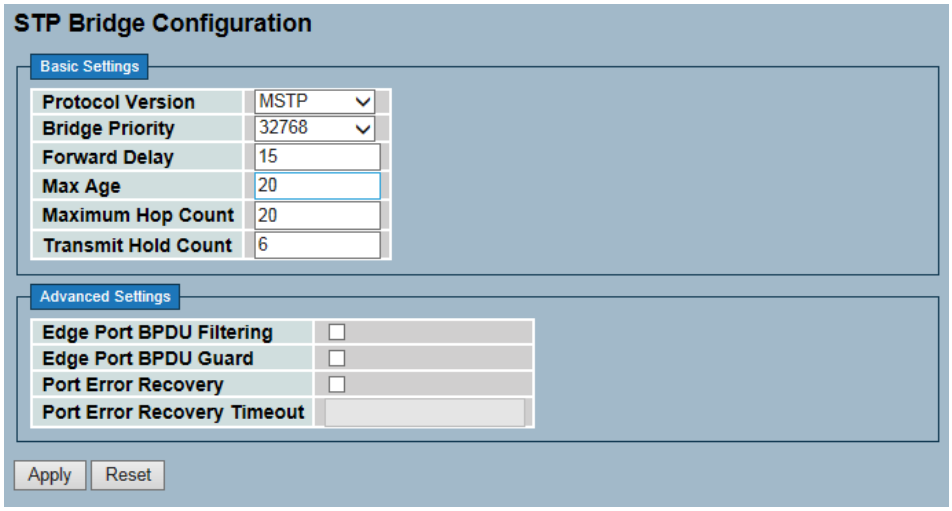


Figure 3-4.1: The STP Bridge Configuration

Parameter Description

Basic Settings

Protocol Version: The STP protocol version setting. Valid values are STP, RSTP, and MSTP.

Bridge Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay: The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age: The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count: This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count: The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering: Controls whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard: Controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery: Controls whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

3-4.2 MSTI Mapping

MSTI Mapping is when you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping because it will receive the VLANs not explicitly mapped. Due to this reason, you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should be left empty (e.g. not having any VLANs mapped to it).

This section allows the user to inspect and change the current STP MSTI bridge instance priority configuration.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specifies the configuration identification parameters in the field. Specifies the VLANs Mapped blank field.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

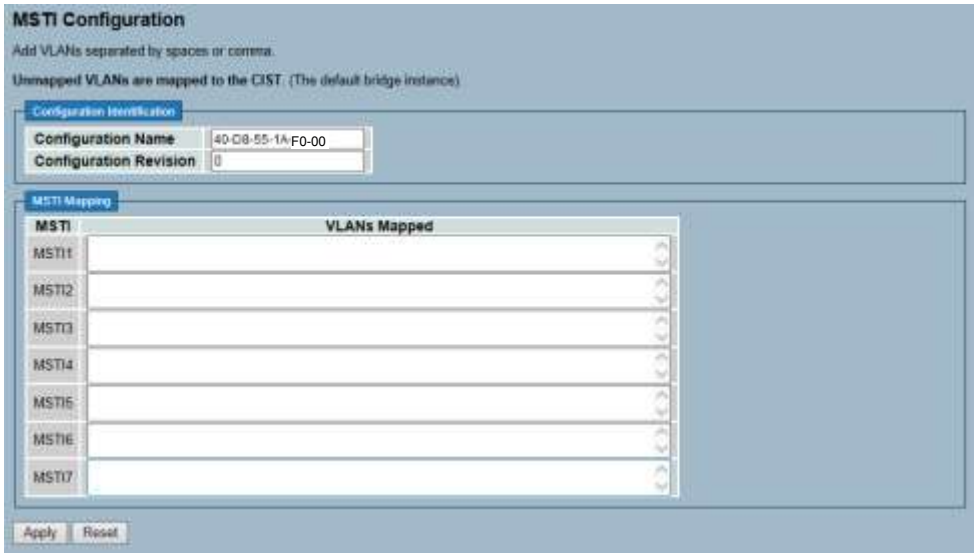


Figure 3-4.2: The MSTI Configuration

Parameter Description

Configuration Identification

Configuration Name: Configuration Name is the name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), and the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI: The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (e.g. not having any VLANs).

3-4.3 MSTI Priorities

When you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance and is always active. For controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

The section allows the user to inspect and change the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Scroll the Priority maximum is 240. Default is 128.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

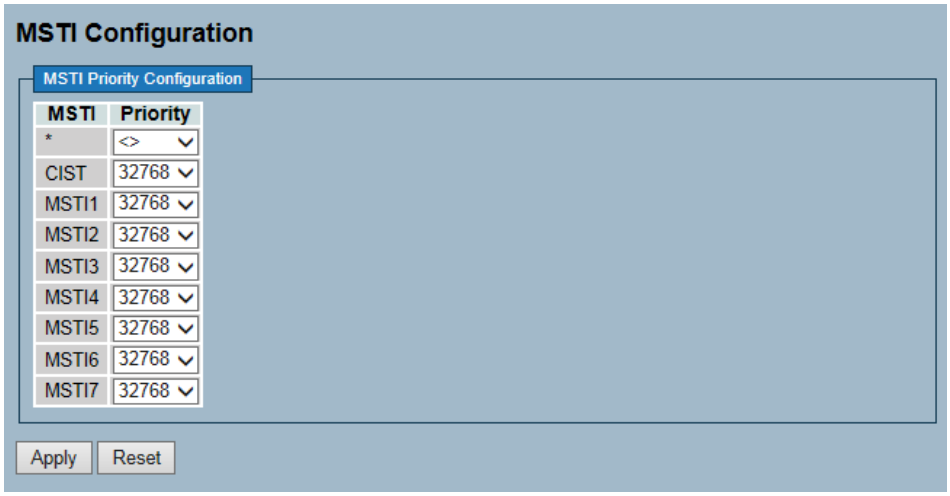


Figure 3-4.3: The MSTI Configuration

Parameter Description

MSTI: The bridge instance. The CIST is the default instance. It is always active.

Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

3-4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance, you need to configure the CIST Ports. The section allows the user to inspect and change the current STP CIST port configurations.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, CIST Ports.
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scroll and evoke to set all parameters of the CIST normal Port configuration.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

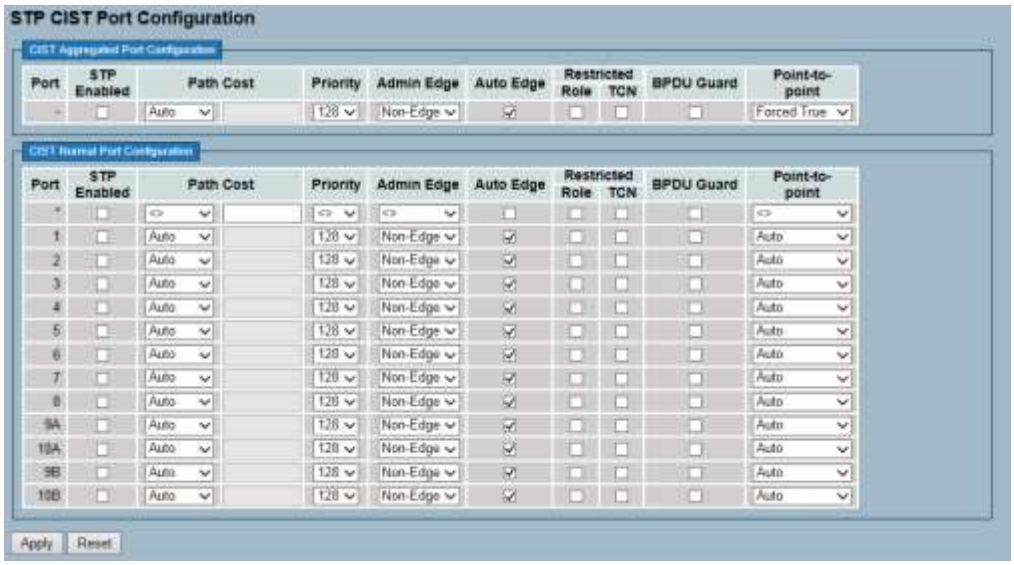


Figure 3-4.4: The STP CIST Port Configuration

Parameter Description

Port: The switch port number of the logical STP port.

STP Enabled: Controls whether STP is enabled on this switch port.

Path Cost: Controls the path cost incurred by the port. The “Auto” setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the “Specific” setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

AdminEdge: Controls whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).

AutoEdge: Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role: If enabled, it causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN: If enabled, it causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard: If enabled, it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.

A port, entering error-disabled state due to this setting, is also subject to the bridge Port Error Recovery setting.

Point to Point: Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

3-4.5 MSTI Ports

The section allows the user to inspect and change the current STP MSTI port configurations.

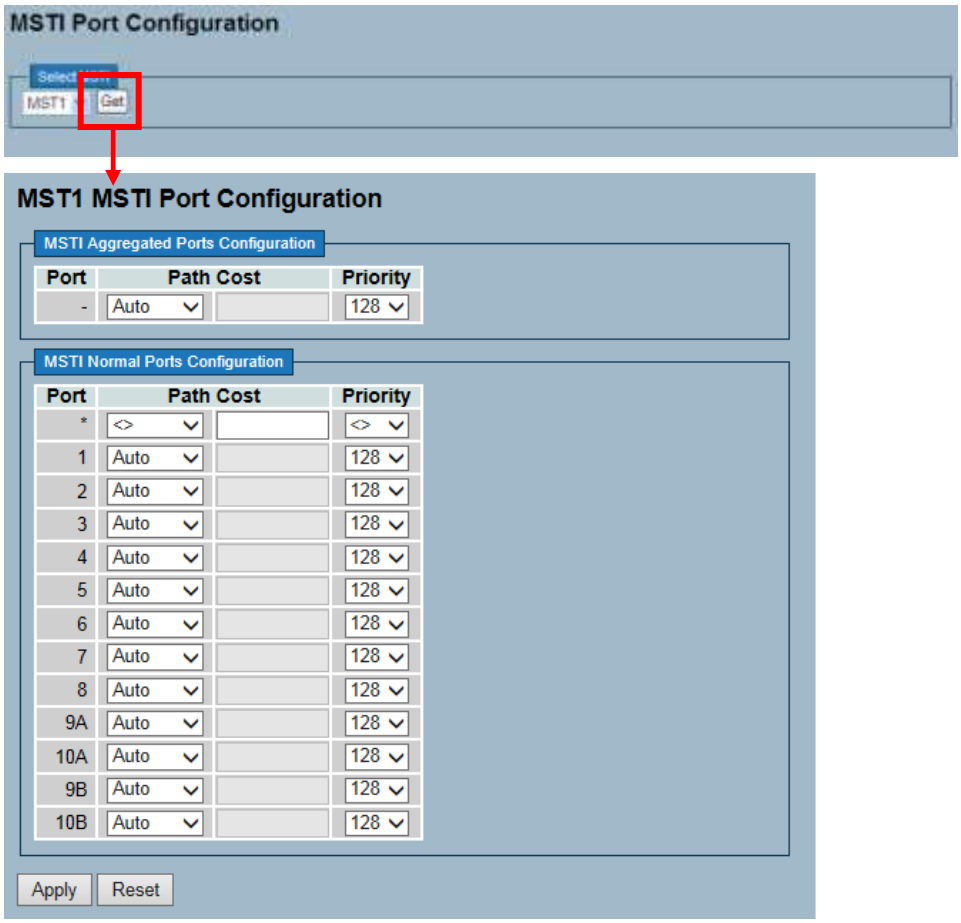
An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports.
2. Scroll to select the MST1 or other MSTI Port.
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click “Save” to save the setting.
6. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Figure 3-4.5: The MSTI Port Configuration



Parameter Description

Port: The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost: Controls the path cost incurred by the port. The auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the “Specific setting”, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert to previously saved values.

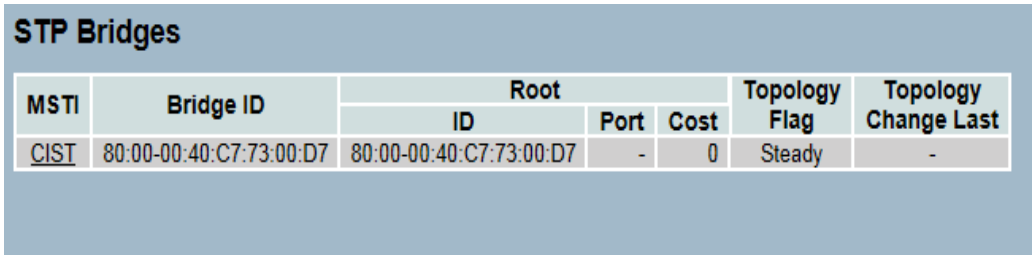
3-4.6 Bridge Status

After the MSTI Port configuration is completed, the switch can now display the Bridge Status. The section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges status in the web interface:

1. Click Configuration, Spanning Tree, and Bridges status.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Click "Refresh" to refresh the STP Bridges.



STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:40:C7:73:00:D7	80:00-00:40:C7:73:00:D7	-	0	Steady	-

Figure 3-4.6: The STP Bridges status

Parameter Description

MSTI: The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID: The Bridge ID of this Bridge instance.

Root ID: The Bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: Root Path Cost. For the Root Bridge it is zero. For all other bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag: The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last: The time since last Topology Change occurred.

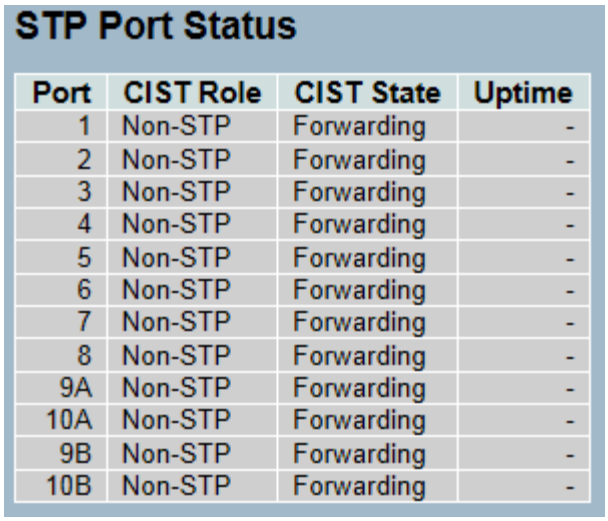
3-4.7 Port Status

After the STP configuration is completed, the switch can now display the STP Port Status. The section provides the STP CIST port status for physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Configuration, Spanning Tree, Port Status.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Click "Refresh" to refresh the STP Bridges.



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9A	Non-STP	Forwarding	-
10A	Non-STP	Forwarding	-
9B	Non-STP	Forwarding	-
10B	Non-STP	Forwarding	-

Figure 3-4.7: The STP Port status

Parameter Description

Port: The switch port number of the logical STP port.

CIST Role: The current STP port role of the CIST port. The port role can be one of the following values: Alternate Port Backup, Port Root, Port Designated, or Port Disabled.

CIST State: The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning, Forwarding.

Uptime: The time since the bridge port was last initialized.

3-4.8 Port Statistics

After the STP configuration is completed, the switch can now display the STP Statistics. The section provides the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Configuration, Spanning Tree, Port Statistics.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Click "Refresh" to refresh the STP Bridges.

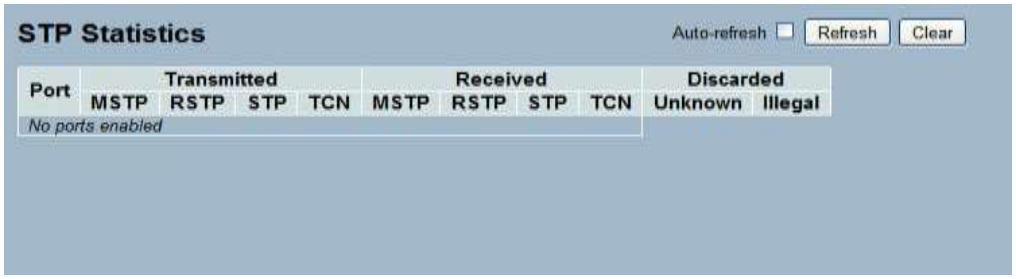


Figure 3-4.8: The STP Statistics

Parameter Description

Port: The switch port number of the logical STP port.

MSTP: The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP: The number of RSTP Configuration BPDU's received/transmitted on the port.

STP: The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN: The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown: The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal: The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

3-5 IGMP Snooping

The function is used to establish the multicast groups to forward the multicast packet to the member ports. It also avoid wasting bandwidth while IP multicast packets are running over the network. This happens because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave. It is a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host. It can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. Once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

3-5.1 Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IGMP Snooping, Basic Configuration.
2. Evoke to select enable or disable which Global configuration.
3. Evoke which port wants to become a Router Port or enable/disable the Fast Leave function.
4. Scroll to set the “Throttling” parameter.
5. Click “Save” to save the setting.
6. If you want to cancel the setting, click the reset button to revert back to previously saved values.

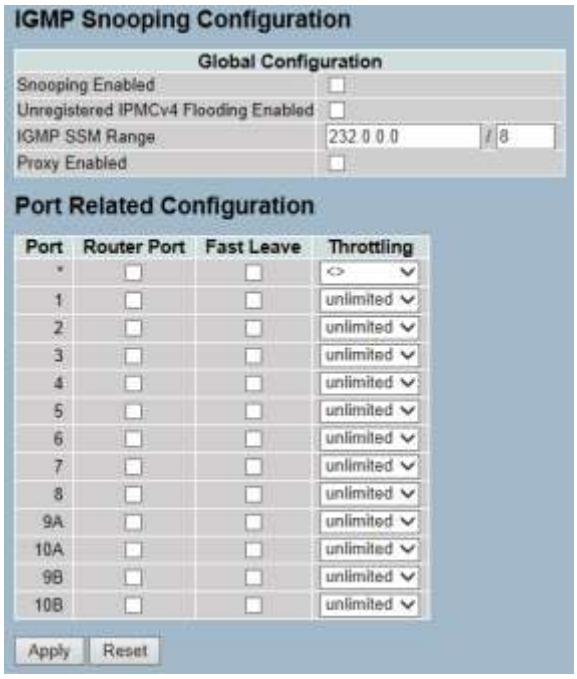


Figure 3-5.1: The IGMP Snooping Configuration.

Parameter Description

Snooping Enabled: Enables the Global IGMP Snooping.

Unregistered IPMC Flooding enabled: Enables unregistered IPMC traffic flooding.

IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Format: (IP address/ sub mask).

Proxy Enabled: Enables IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port: Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enables the fast leave on the port.

Throttling: Enables to limit the number of multicast groups to which a switch port can belong.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-5.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. Each setting page shows up to 99 entries from the VLAN table. The default is 20 and can be selected through the "entries per page" input field. During the initial visit, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table, starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IGMP Snooping, and VLAN Configuration.
2. Evoke to select enable or disable Snooping, IGMP Querier. Specify the parameters in the blank field.
3. Click the refresh to update the data or click **<<** or **>>** to display previous entry or next entry.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

Figure 3-5.2: The IGMP Snooping VLAN Configuration.

Parameter Descriptions

VLAN ID: This displays the VLAN ID of the entry.

Snooping Enabled: Enables the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.

IGMP Querier: A router sends IGMP Query messages onto a particular link. This Router is called the Querier. Enables the IGMP Querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions, depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

Rv: Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255. The default robustness variable value is 2.

QI: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.

QRI: Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds. The default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds. The default last member query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds. The default unsolicited report interval is 1 second.

Buttons:

- **Apply** – Click to apply changes.
- **Reset-** Click "Reset" to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh, |<<, >>): You can click the icons to refresh the displayed table starting from the "VLAN" input fields. Or click "**|<<**" to update the table, starting from the first entry in the VLAN table (e.g. the entry with the lowest VLAN ID). Click "**>>**" to update the table, starting with the entry after the last entry currently displayed.

3-5.3 Port Group Filtering

The section describes how to set the IGMP Port Group Filtering. With the IGMP filtering feature, an user can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, an user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups. It can specify whether access to the group is permitted or denied. If an IGMP profile denies access to a multicast group on a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the web interface:

1. Click Configuration, IGMP Snooping, Port Group Filtering.
2. Click Add new Filtering Group.
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

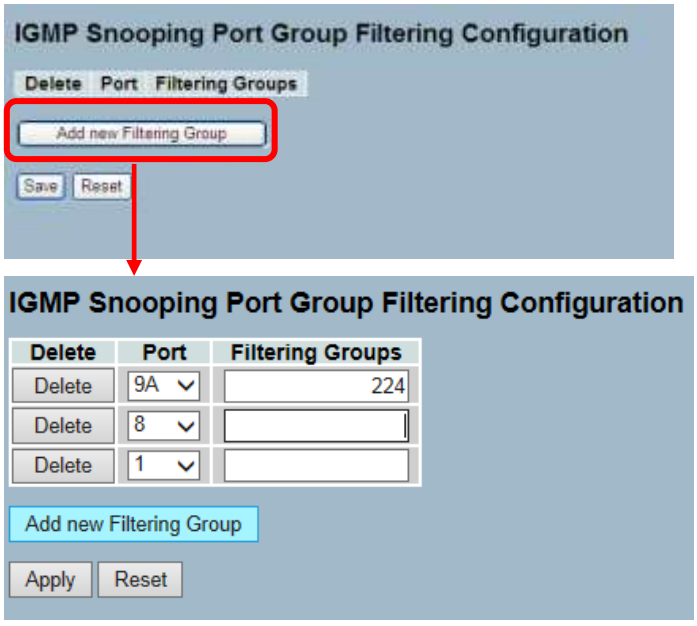


Figure 3-5.3: The IGMP Snooping Port Group Filtering Configuration

Parameter Descriptions

Delete: Check to delete the entry. It will be deleted during the next save.

Port: To evoke the port enable the IGMP Snooping Port Group Filtering function.

Filtering Groups: The IP Multicast Group that will be filtered.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-5.4 Status

After the IGMP Snooping configuration is completed, the switch can display the IGMP Snooping Status. The section provides the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Configuration, IGMP Snooping, Status.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh” to refresh the IGMP Snooping Status.
4. Click “ Clear“ to clear the IGMP Snooping Status.

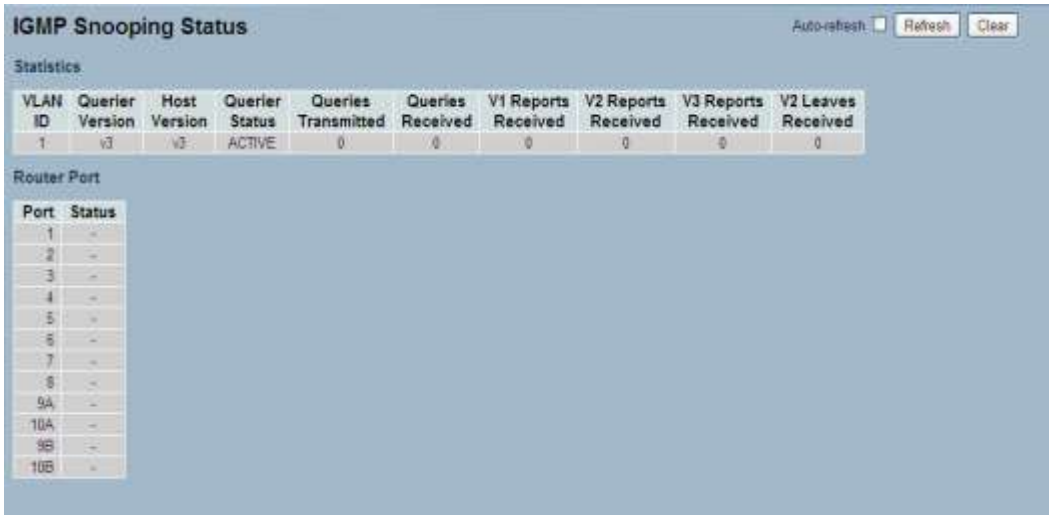


Figure 3-5.4: The IGMP Snooping Status.

Parameter Descriptions

VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Current Working Host Version.

Querier Status: Shows the Querier status is "ACTIVE" or "IDLE".

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Port: Switch port number.

Status: Indicates whether specific port is a router port or not.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, clear): Click “Refresh” to refresh the status or clear them manually.

3-5.5 Group Information

After the IGMP Snooping function setting is completed, the switch can display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID and then by group. The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No more entries" appears. Use the button to start over.

Web Interface

To display the IGMP Snooping Group Information in the web interface:

1. Click Configuration, IGMP Snooping, Group Information.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh” to refresh a entry of the IGMP Snooping Groups Information.
4. Click **“<< or >>”** to move to previous or next entry.

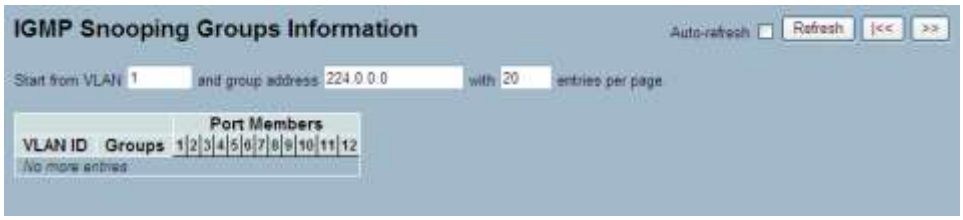


Figure 3-5.5: The IGMP Snooping Groups Information.

Parameter Description

Navigating the IGMP Group Table

The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the IGMP Group Table. The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No More Entries" appears.

IGMP Group Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the IGMP Group Status manually. Click **“<<”** or **“>>”** to move to the next or previous page.

3-5.6 IPV4 SSM Information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host indicates that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses too.

Web Interface

To display the IGMPv3 IPv4 SSM Information in the web interface:

1. Click Configuration, IGMP Snooping, IPv4 SSM Information.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Click "Refresh" to refresh a entry of the IGMPv3 IPv4 SSM Information.
4. Click "**<< or >>**" to move to previous or next entry.

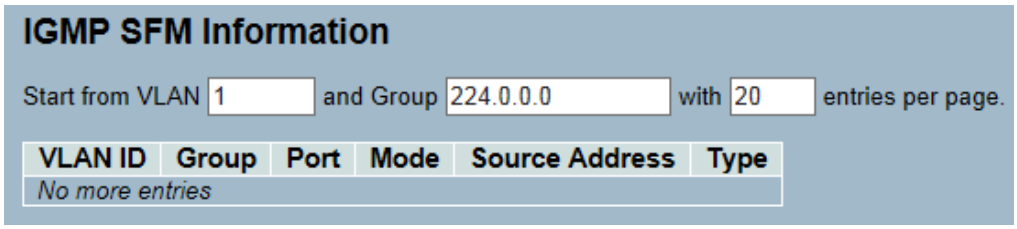


Figure 3-5.6: The IGMPv3 IPv4 SSM Information.

Parameter Description

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) Information Table. The default is 20. This can be selected through the "entries per page" input field. During the initial visit, the web page will show the first 20 entries from the beginning of the IGMPv3 Information Table.

The "Start from VLAN", and "Group" input fields allow the user to select the starting point in the IGMPv3 Information Table. Clicking the button will update the displayed table, starting from that or the closest next IGMPv3 Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry to allow continuous refresh with the same start address.

The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "No More Entries" appears. Use the button to start over.

IGMPv3 Information Table Columns

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either Allow or Deny.

Auto-refresh: To evoke the auto-refresh icon, then the device will refresh the log automatically.

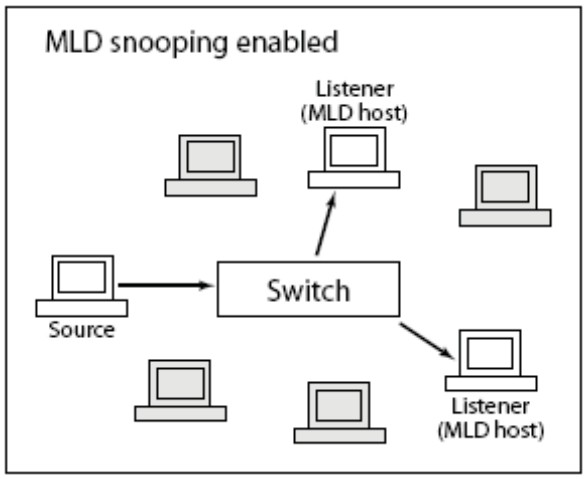
Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the IGMP Group Status manually. Click **“<<”** or **“>>”** to move to the next or previous page.

3-6 MLD Snooping

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping. It provides multicast traffic and MLD doesn't interact with it. Please note that in an application, like desktop conferencing, a network node may act as both a source and an MLD host. However, MLD interacts with that node only in its role as an MLD host.

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (e.g. "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. This is a function of the application software, not of MLD.

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic to ports on the VLAN that have MLD hosts for that address. It drops traffic for ports on the VLAN that have no MLD hosts.



3-6.1 Basic Configuration

The section helps you configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, MLD Snooping, Basic Configuration.
2. Evoke to enable or disable the Global configuration parameters. Evoke the port to join Router Port and Fast Leave.
3. Scroll to select the Throttling mode with unlimited or 1 to 10.
4. Click "Save" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

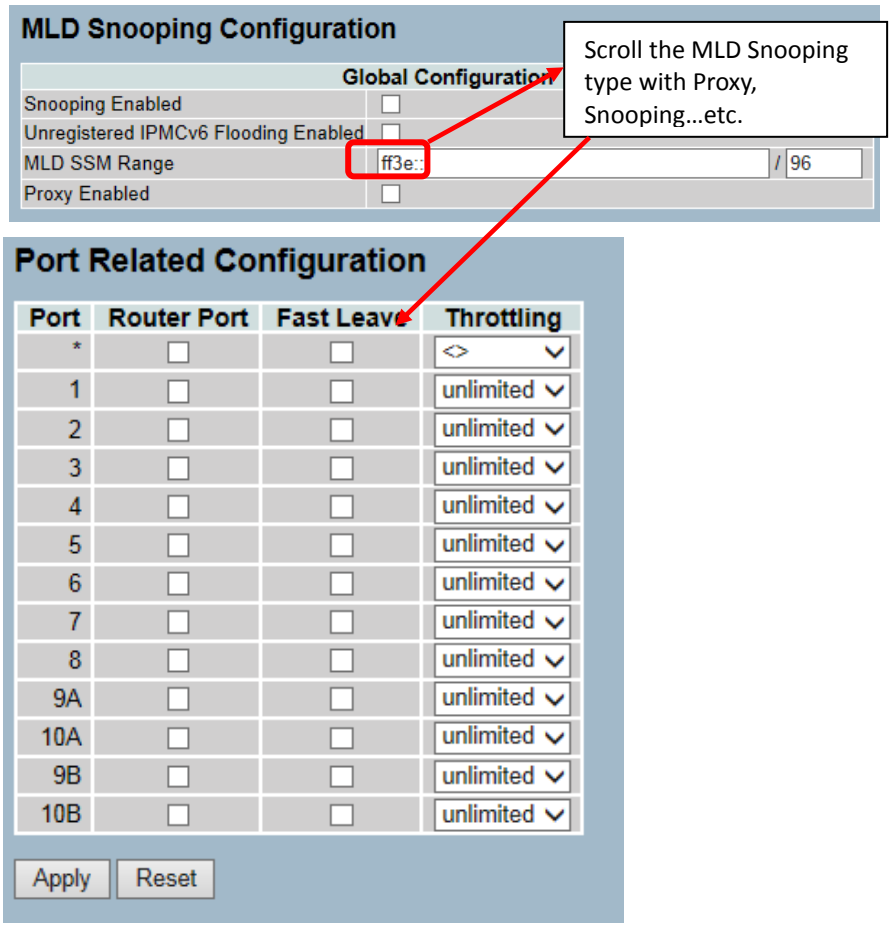


Figure 3-6.1: The MLD Snooping Basic Configuration

Parameter Description

Snooping Enabled: Enables the Global MLD Snooping.

Unregistered IPMC Flooding enabled: Enables unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.

MLD SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address (using IPv6 Address) range.

Proxy Enabled: Enables MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: The Port index what you enable or disable the MLD Snooping function.

Router Port: Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: To evoke to enable the fast leave on the port.

Throttling: Enables to limit the number of multicast groups to which a switch port can belong.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-6.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch minimizes unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic to ports on the VLAN that have MLD hosts for that address. It drops traffic for ports on the VLAN that have no MLD hosts.

The switch will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text "No More Entries" appears. Use the button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

1. Click Configuration, MLD Snooping, VLAN Configuration.
2. Specify the VLAN ID with entries per page.
3. Click “Refresh” to refresh a entry of the MLD Snooping VLAN Configuration Information.
4. Click “**<< or >>**” to move to previous or next entry.

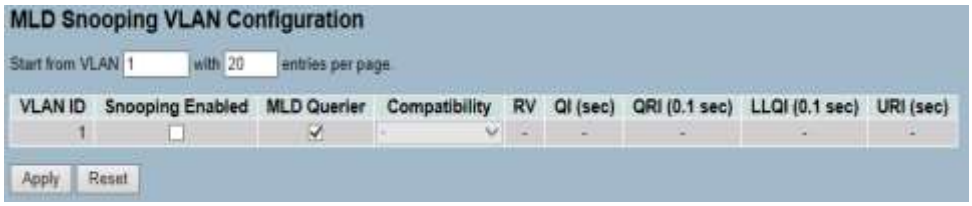


Figure 3-6.2: The MLD Snooping VLAN Configuration.

Parameter Description

VLAN ID: The VLAN ID of the entry.

Snooping Enabled: Enables the per-VLAN MLD Snooping. Only up to 32 VLANs can be selected.

MLD Querier: A router sends MLD Query messages onto a particular link. This Router is called the Querier. It enables the MLD Querier in the VLAN.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions, depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, and Forced MLDv2. The default compatibility value is MLD-Auto.

Rv: Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255. The default robustness variable value is 2.

QI: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.

QRI: Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds. The default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries. It is sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds. The default last listener query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds. The default unsolicited report interval is 1 second.

Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the IGMP Group Status manually. Click **“<<”** or **“>>”** to move to the next or previous page.

Buttons:

- **Apply** – Click to apply changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-6.3 Port Group Filtering

The section describes how to set up the Port Group Filtering in the MLD Snooping function. On the UI, you could add new filtering group and safety policy.

Web Interface

To configure the MLD Snooping Port Group Configuration in the web interface:

1. Click Configuration, MLD Snooping, Port Group Filtering Configuration.
2. Click the Add new Filtering Group.
3. Specify the Filtering Groups with entries per page.
4. Click "Save" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

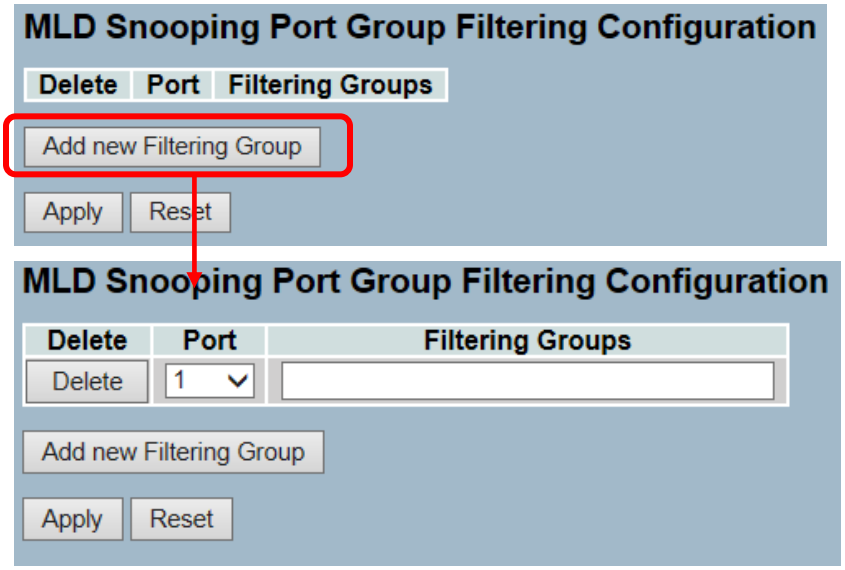


Figure 3-6.3: The MLD Snooping Port Group Filtering Configuration

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings. You can evoke to enable the port to join filtering Group

Filtering Groups: The IP Multicast Group that will be filtered.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset-** Click "Reset" to undo any changes made locally and revert to previously saved values.

3-6.4 Status

The section describes how to display the MLD Snooping Status and detail information after completing the MLD Snooping. It will help you find the detail information of MLD Snooping status.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Configuration, MLD Snooping, Status.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh” to refresh a entry of the MLD Snooping Status Information.
4. Click “ Clear“ to clear the MLD Snooping Status.

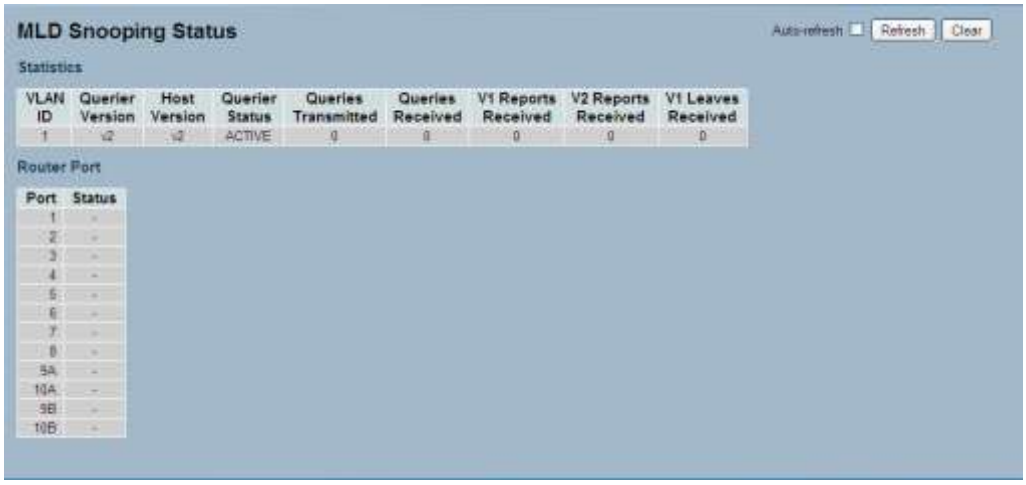


Figure 3-6.4: The MLD Snooping Status

Parameter Description

VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Current working Host Version.

Querier Status: Shows the Querier status is "ACTIVE" or "IDLE".

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V1 Leaves Received: The number of Received V1 Leaves.

Port: Switch port number.

Status: Indicates whether specific port is a router port or not.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the IGMP Group Status manually. Click **“<<”** or **“>>”** to move to the next or previous page.

3-6.5 Group Information

The section describes how to set up the MLD Snooping Groups Information. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLD Group Table.

Each page shows up to 99 entries from the MLD Group table. The default is 20 and can be selected through the "Entries Per Page" input field. During the initial visit, the web page will show the first 20 entries from the beginning of the MLD Group Table.

Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Configuration, MLD Snooping, Group Information.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh” to refresh a entry of the MLD Snooping Group Information.
4. Click “ Clear“ to clear the MLD Snooping Groups information.

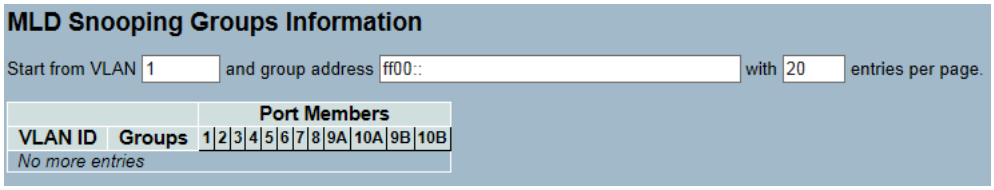

MLD Snooping Groups Information
Start from VLAN 1 and group address ff00:: with 20 entries per page.
Port Members
VLAN ID Groups 1 2 3 4 5 6 7 8 9A 10A 9B 10B
No more entries

Figure 3-6.5: The MLD Snooping Groups Information

Parameter Description

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table. The default is 20 and can be selected through the “Entries Per Page “ input field. During the initial visit, the web page will show the first 20 entries from the beginning of the MLD Group Table. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table, starting from that or the next closest.

MLD Group Table Match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry to allow continuous refresh with the same start address. The switch will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached, the text “No More Entries” appears. Use the button to start over.

MLD Snooping Information Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the log automatically.

Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the IGMP Group Status manually. Click **“<<”** or **“>>”** to move to the next or previous page.

3-6.6 IPV6 SSM Information

The section configures the Entries in the MLDv2 Information Table. The MLDv2 Information Table is sorted first by VLAN ID, by Group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLDv2 SSM (Source Specific Multicast) Information Table. The default is 20 and can be selected through the "Entries Per Page" input field. During the initial visit, the web page will show the first 20 entries from the beginning of the MLDv2 Information Table. The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the MLDv2 Information Table.

Web Interface

To display the MLDv2 IPv6 SSM Information in the web interface:

1. Click Configuration, MLD Snooping, IPv6 SSM Information.
2. If you want to auto-refresh the information, then you need to evoke the “Auto-Refresh”.
3. Click “Refresh” to refresh a entry of the MLDv2 IPv6 SSM Information.
4. Click **“<< or >>”** to move to previous or next entry.

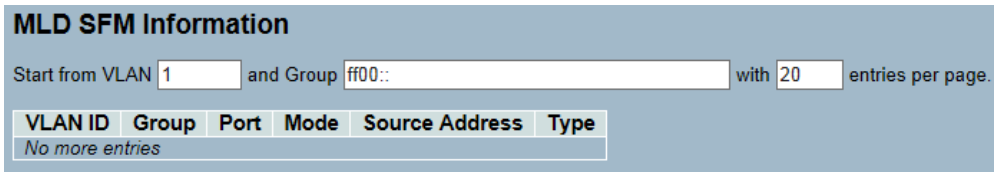

MLD SFM Information
Start from VLAN 1 and Group ff00:: with 20 entries per page.
VLAN ID Group Port Mode Source Address Type
No more entries

Figure 3-6.6: The IPv6 SSM Information

Parameter Description

MLDv2 Information Table Columns

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either Allow or Deny.

3-7 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box, can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

3-7.1 Configuration

The section describes how the user could set the MVR basic conifguration and some parameters on the switch.

Web Interface

To configure the MLD Snooping Port Group Configuration in the web interface:

1. Click Configuration, MVR, Configuration.
2. Scroll the MVR mode to enable or disable and scroll to set all parameters.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

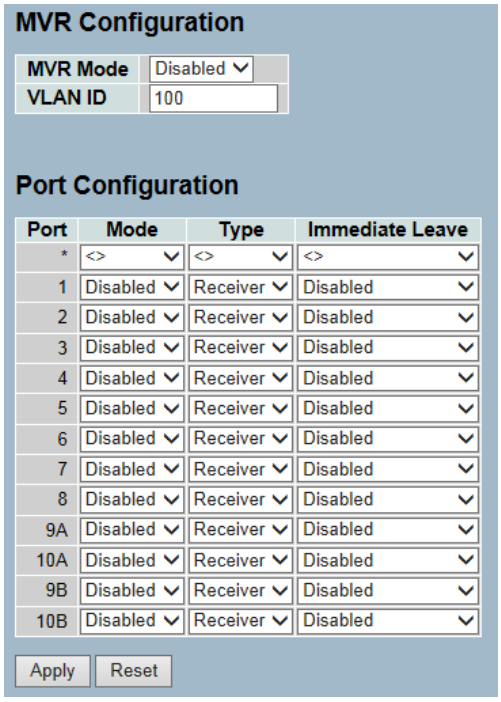


Figure 3-7.1: The MVR Configuration

Parameter Description

MVR Mode: Enables/Disables the Global MVR.

VLAN ID: Specifies the Multicast VLAN ID.

Mode: Enables MVR on the port.

Type: Specifies the MVR port type on the port.

Immediate Leave: Enables the fast leave on the port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-7.2 Port Group Allow

The section describes how to allow the IP Multicast Group to receive the multicast stream. Entries in the MVR port group allow table is shown on this page. The MVR Port Group Table is sorted first by port and then by IP address.

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Configuration, MVR, Port Groups Allow.
2. If you want to add the new allowed group, you need to click the “Add New Allow Group” button.
3. Evoke the “Port No.”, “Start Address” and “End Address”.
4. To click the “Apply” to apply the configuration of MVR Port Group Allow Table.

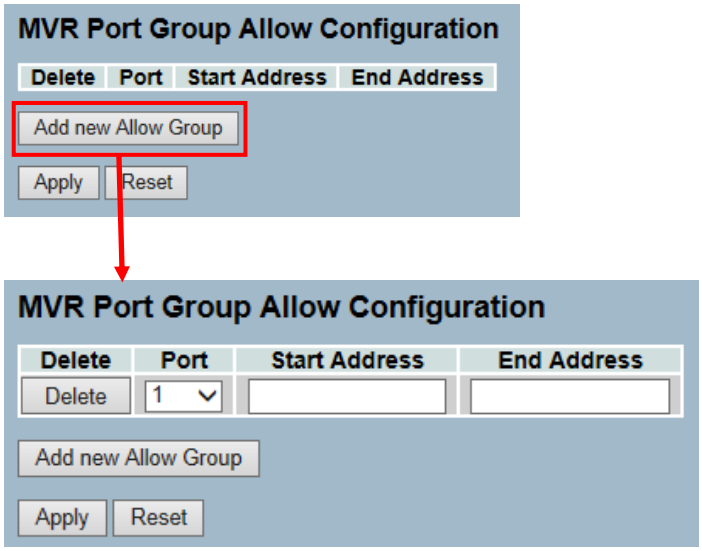


Figure 3-7.2: The MVR Groups Information

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next apply.

Port: The logical port for the settings.

Allow Groups: The IP Multicast Group that will be allowed.

Adding New Allow Group: Click “Add New Allow Group” to add a new entry to the Group Allow table. Specifies the Port and Allow Group of the new entry. Click "Apply".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-7.3 Groups Information

The section describes how to display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID and then by group.

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Configuration, MVR, Groups Information.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. To Click the "Refresh" to refresh a entry of the MVR Groups Information.
4. Click **"<< or >>"** to move to previous or next entry.

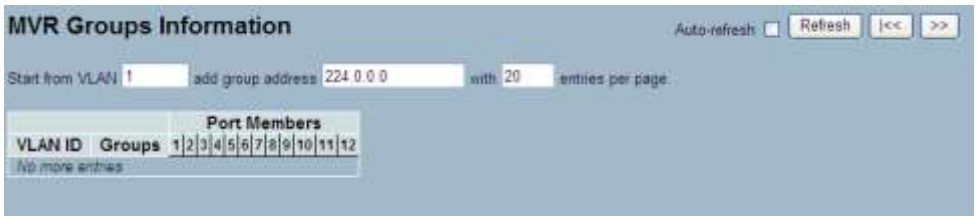


Figure 3-7.2: The MVR Groups Information

Parameter Description

MVR Group Table Columns

VLAN ID: VLAN ID of the group.

Groups: Group ID of the group displayed.

Port Members: Ports under this group.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click "Refresh" to refresh the MVR Group information manually. Click **"<<"** or **">>"** to move to the next or previous page.

3-7.4 Statistics

The section describes how to display the MVR detail statistics after the MVR is configured on the switch. It provides the detail MVR Statistics Information.

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Configuration, MVR, Statistics.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. To Click the "Refresh" to refresh a entry of the MVR Statistics Information.
4. Click **"<< or >>"** to move to previous or next entry.

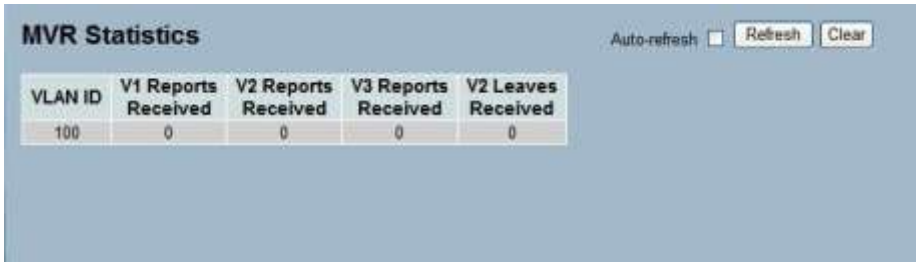


Figure 3-7.4: The MVR Statistics Information

Parameter Description

VLAN ID: The Multicast VLAN ID.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Auto-refresh: Check "Auto-Refresh" so the device can refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click "Refresh" to refresh the MVR Group information manually. Click **"<<"** or **">>"** to move to the next or previous page.

3-8 LLDP

The switch supports LLDP. For current information on your switch model, the Link Layer Discovery Protocol (LLDP) provides a standards-based method. This method enables switches to advertise themselves to adjacent devices and learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite. It is used by network devices to advertise their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery, specified in standards document IEEE 802.1AB.

3-8.1 LLDP Configuration

You can set up the LLDP configuration and detail parameters per port. The settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click LLDP configuration.
2. Modify LLDP timing parameters.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click “Apply”.

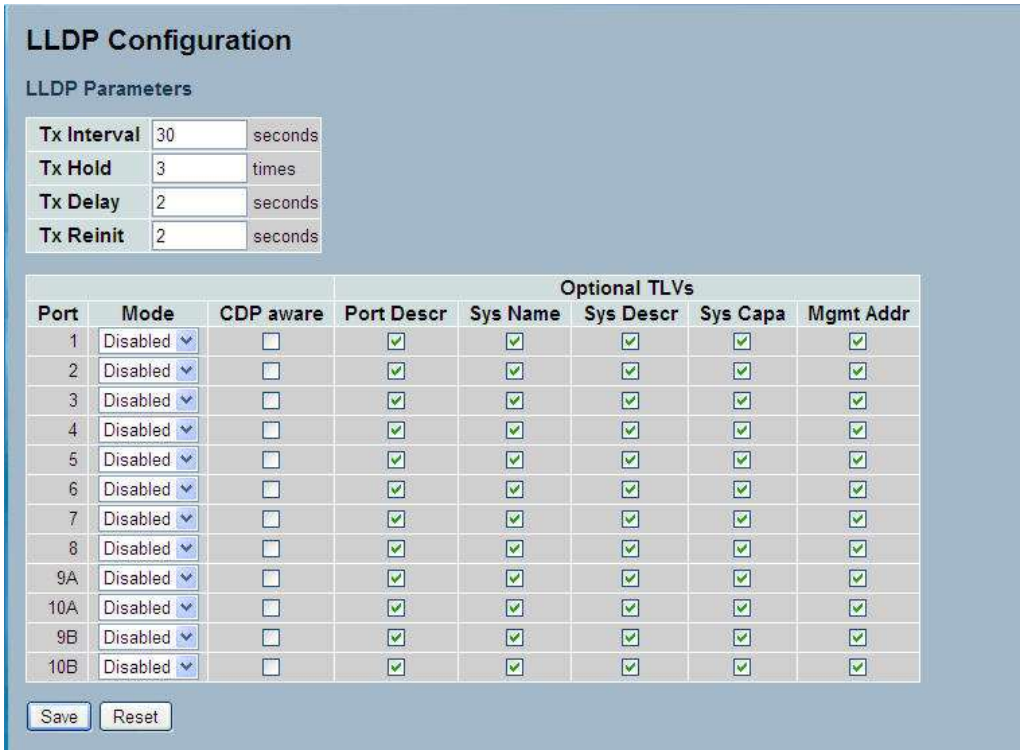


Figure 3-8.1: The LLDP Configuration

Parameter Description

LLDP Parameters

Tx Interval: The switch periodically transmits LLDP frames to its neighbors to keep the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 to 32768 seconds.

Tx Hold: Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay: If some configurations changed (e.g. the IP address), a new LLDP frame is transmitted. However, the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit: When a port is disabled, LLDP is disabled or the switch is rebooted. A LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Port: The switch port number of the logical LLDP port.

Mode: Select LLDP mode.

- **Rx only**: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
- **Tx only**: The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- **Disabled**: The switch will not send out LLDP information and will drop LLDP information received from neighbors.
- **Enabled**: The switch will send out LLDP information and will analyze LLDP information received from neighbors.

CDP Aware: Select CDP awareness.

- The CDP operation is restricted to decoding incoming CDP frames (the switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.
- Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics). CDP TLVs are mapped onto LLDP neighbors' table as shown below.
- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
- Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.
- If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.

NOTE: When CDP awareness on a port is disabled the CDP information isn't removed immediately. It gets removed when the hold time is exceeded.

Port Descr: Optional TLV: When checked, the "port description" is included in LLDP information transmitted.

Sys Name: Optional TLV: When checked, the "system name" is included in LLDP information transmitted.

Sys Descr: Optional TLV: When checked, the "system description" is included in LLDP information transmitted.

Sys Capa: Optional TLV: When checked, the "system capability" is included in LLDP information transmitted.

Mgmt Addr: Optional TLV: When checked, the "management address" is included in LLDP information transmitted.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-8.2 LLDP Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

Web Interface

To show LLDP neighbors:

1. Click LLDP Neighbors.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

Figure 3-8.2: The LLDP Neighbors information

NOTE: If your network without any device supports LLDP, then the table will show “No LLDP Neighbor Information Found”.

Parameter Description

Local Port: The port on which the LLDP frame was received.

Chassis ID: The chassis ID is the identification of the neighbor's LLDP frames.

Remote Port ID: The remote port ID is the identification of the neighbor port.

System Name: System mame is the name advertised by the neighbor unit.

Port Description: Port description is the port description advertised by the neighbor unit.

System Capabilities: System capabilities describe the neighbor unit's capabilities. The possible capabilities are:

- Other
- Repeater
- Bridge
- WLAN Access Point
- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

System Description: Port description is the port description advertised by the neighbor unit.

Management Address: Management address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could hold the neighbor's IP address.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the LLDP neighbors information manually.

3-8.3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, also known as LLDP-MED, that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services – Diffserv - settings) enable plug and play networking.

Device location discovery allows creation of location databases and in the case of Voice over Internet Protocol (VoIP), enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

Inventory management allows network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices, which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click LLDP-MED Configuration.
2. Modify Fast start repeat count parameter. The default is 4.
3. Modify Coordinates Location parameters.
4. Fill Civic Address Location parameters.
5. Add new policy.
6. Click “Apply”. It will show the Policy Port Configuration.
7. Select Policy ID for each port.
8. Click “Apply”.

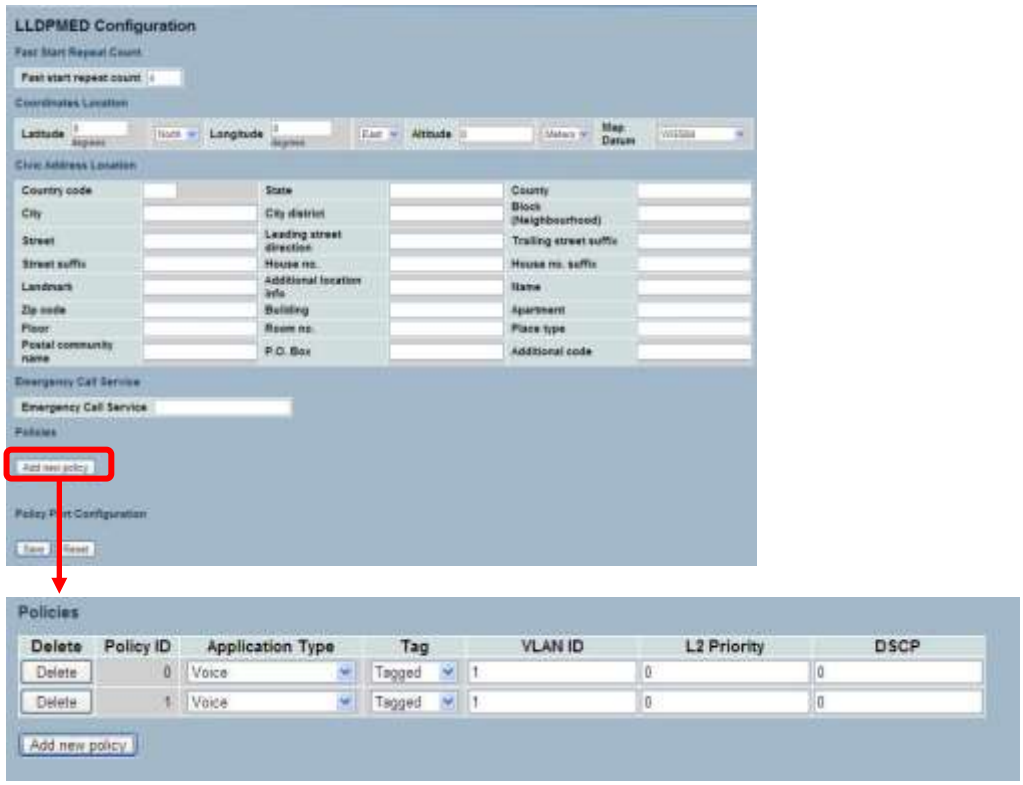


Figure 3-8.3: The LLDP-MED Configuration

Parameter Description

Fast start repeat count

Rapid Startup and Emergency Call Service Location Identification Discovery of endpoints are critical aspects of VoIP systems. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (e.g. only advertise the voice network policy to permitted voice-capable devices). This conserves the limited LLDPU space, and reduces security and system integrity issues that can come with inappropriate knowledge of the network policy.

LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will a LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of losing a LLDP frame during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With fast start repeat count, it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times when an LLDP frame with new information is received, given that 4 LLDP frames with a 1 second interval will be transmitted.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices. It does not apply to links between LAN infrastructure elements, including Network Connectivity Devices or other types of links.

Coordinates Location

Latitude: Latitude **should** be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude: Longitude **should** be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude: Altitude **should** be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

- **Meters**: Represents meters of altitude defined by the vertical datum specified.
- **Floors**: Represents altitude in a form more relevant in buildings, which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building. It represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum: The Map Datum is used for the coordinates given in these options:

- **WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
- **NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
- **NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country code: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State: National subdivisions (state, canton, region, province, prefecture)

County: County, parish, gun (Japan), district.

City: City, township, shi (Japan) - Example: Copenhagen

City district: City division, borough, city district, ward, chou (Japan)

Block (Neighborhood): Neighborhood, block

Street: Street - Example: Poppelvej

Leading street direction: Leading street direction - Example: N

Trailing street suffix: Trailing street suffix - Example: SW

Street suffix: Street suffix - Example: Ave, Platz

House no.: House number - Example: 21

House no. suffix: House number suffix - Example: A, 1/2

Landmark: Landmark or vanity address - Example: Columbia University

Additional location info: Additional location info - Example: South Wing

Name: Name (residence and office occupant) - Example: Flemming Jahn

Zip code: Postal/zip code - Example: 2791

Building: Building (structure) - Example: Low Library

Apartment: Unit (Apartment, suite) - Example: Apt 42

Floor: Floor - Example: 4

Room no.: Room number - Example: 450F

Place type: Place type - Example: Office

Postal community name: Postal community name - Example: Leonia

P.O. Box: Post office box (P.O. BOX) - Example: 12345

Additional code: Additional code - Example: 1320300003

Emergency Call Service: Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

- Layer 2 VLAN ID (IEEE 802.1Q-2003)
- Layer 2 priority value (IEEE 802.1D-2004)
- Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

- Voice
- Guest Voice
- Softphone Voice
- Video Conferencing
- Streaming Video
- Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints. Therefore, it does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete: Check to delete the policy. It will be deleted during the next save.

Policy ID: ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.

Application Type: Intended use of the application types:

- **Voice** - For use by dedicated IP Telephony handsets and other similar appliances that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
- **Voice Signaling** (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
- **Guest Voice** - Supports a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances that support interactive voice services.
- **Guest Voice Signaling** (conditional) - For use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
- **Softphone Voice** - For use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
- **Video Conferencing** - For use by dedicated video conferencing equipment and other similar appliances that support real-time interactive video/audio services.
- **Streaming Video** - For use by broadcast or multicast based video content distribution and other similar applications that support streaming video services and require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
- **Video Signaling** (conditional) - For use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply to those advertised in the video conferencing application policy.

Tag: Tag indicates whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format. Both the VLAN ID and the Layer 2 priority values are also used, as well as, the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID: VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP: DSCP value to be used to provide Diffserv node behavior for the specified application type, as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value, as defined in RFC 2475.

Adding a new policy: Click to add a new policy. Specify the application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".

Port Policies Configuration: Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port: The port number to which the configuration applies.

Policy Id: The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-8.4 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Web Interface

To show LLDP-MED neighbors:

1. Click LLDP-MED Neighbors.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

Figure 3-8.4: The LLDP-MED Neighbors information

NOTE: If your network is without any device supports LLDP-MED, then the table will show "No LLDP-MED Neighbor Information Found".

Parameter Description

Port: The port on which the LLDP frame was received.

Device Type: LLDP-MED Devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices.

- LLDP-MED Network Connectivity Device Definition
- LLDP-MED network connectivity devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. A LLDP-MED network connectivity device is a LAN access device based on any of the following technologies:
    1. LAN Switch/Router
    2. IEEE 802.1 Bridge
    3. IEEE 802.3 Repeater (included for historical reasons)
    4. IEEE 802.11 Wireless Access Point
    5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057, and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition: LLDP-MED endpoint devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED endpoint device category, the LLDP-MED scheme is broken into further endpoint device classes, as defined in the following.

Each LLDP-MED endpoint device class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For example, any LLDP-MED endpoint device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I). Any LLDP-MED endpoint device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I): The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057. However, it does not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP communication controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II): The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities. However, it may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice/Media Gateways, Conference Bridges, Media Servers, and similar products.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III): The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management.

LLDP-MED Capabilities: LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type: Application Type indicates the primary function of the application(s) defined for this network policy. It is advertised by an endpoint or network connectivity device. The possible application types are shown below:

1. **Voice** - For use by dedicated IP Telephony handsets and other similar appliances that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signaling** - For use in network topologies that require a different policy for the voice signaling than for the voice media.
3. **Guest Voice** - Supports a separate limited feature – to set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances that support interactive voice services.
4. **Guest Voice Signaling** - For use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
5. **Softphone Voice** - For use by softphone applications on typical data centric devices, such as PCs or laptops.
6. **Video Conferencing** - For use by dedicated video conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
8. **Streaming Video** - For use by broadcast or multicast based video content distribution and other similar applications to support streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
9. **Video Signaling** - For use in network topologies that require a separate policy for the video signaling than for the video media.

Policy: Policy indicates that an endpoint device wants to explicitly advertise that the policy is required by the device. Can be either “Defined” or “Unknown”.

- **Unknown**: The network policy for the specified application type is currently unknown.
- **Defined**: The network policy is defined.

TAG: TAG indicates whether the specified application type is using a tagged or an untagged VLAN. Can be “Tagged” or “Untagged”.

- **Untagged**: The device is using an untagged frame format and does not include a tag header as defined by IEEE 802.1Q-2003.
- **Tagged**: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003. This means that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority: Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contains one of 64 code point values (0 through 63).

3-8.5 EEE

By using EEE, power savings can be achieved at the expense of traffic latency. This latency occurs because the circuits, that EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective TX and RX "wakeup time " as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Web Interface

To show LLDP EEE neighbors:

1. Click LLDP, then click EEE to show discovered EEE devices.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

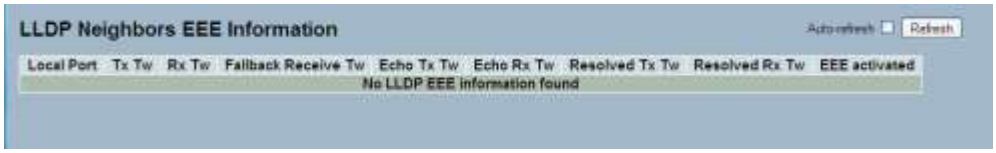


Figure 3-8.5: The LLDP Neighbors EEE information

NOTE: If your network is without any devices, the EEE function will enable and then the table will show “No LLDP EEE Information Found”.

Parameter Description

Local Port: The port on which LLDP frames are received or transmitted.

Tx Tw: The link partner's maximum time to transmit path can hold off sending data after deassertion of LPI.

Rx Tw: The link partner's time that receiver would like the transmitter to hold off, allowing time for the receiver to wake from sleep.

Fallback Receive Tw: The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that may be used for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw: The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partner’s reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner had received, registered, and processed the most recent values. For example, if the local link partner receives echoed parameters that do not match the values in the local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw: The link partner's Echo Rx Tw value.

Resolved Tx Tw: The resolved Tx Tw for this link. Note: It is not the link partner.

The resolved value that is the actual "Tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw: The resolved Rx Tw for this link. Note: It is not the link partner.

The resolved value that is the actual "Tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

EEE activated: Shows if the switch and the link partner have agreed upon which wakeup times to use.

- **Red** - Switch and link partner have not agreed upon wakeup time.
- **Green** - Switch and link partner have agreed upon wakeup time.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the LLDP Neighbors information manually.

3-8.6 Port Statistics

There are two types of counters for port statistics: global counters and local counters. Global counters are counters that refer to the whole stack switch. While local counters refer to per port counters for the currently selected switch.

Web Interface

To show LLDP Statistics:

1. Click LLDP, then click Port Statistics to show LLDP counters.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.
4. Click Clear to clear all counters.

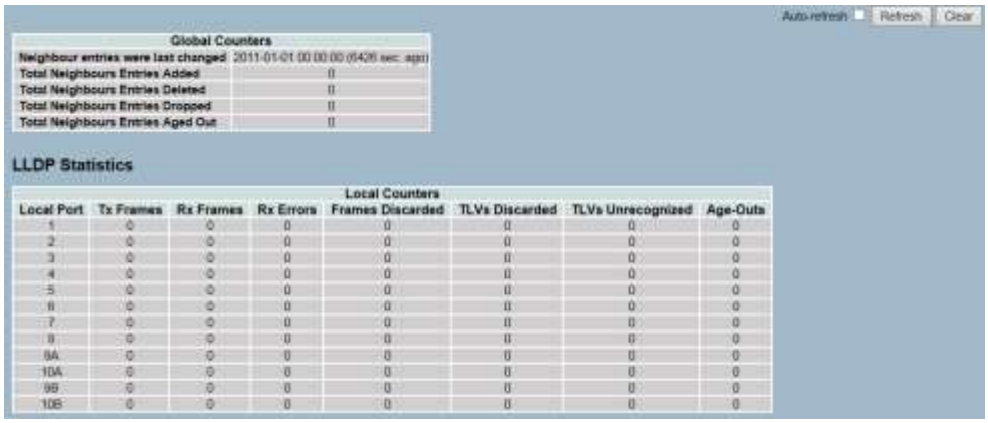


Figure 3-8.6: The LLDP Port Statistics information

Parameter Description

Global Counters

Neighbor entries were last changed: It shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added: Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted: Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped: Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out: Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port: The port on which LLDP frames are received or transmitted.

Tx Frames: The number of LLDP frames transmitted on the port.

Rx Frames : The number of LLDP frames received on the port.

Rx Errors: The number of received LLDP frames containing some kind of error.

Frames Discarded: If an LLDP frame is received on a port and the switch's internal table is full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received or when the entry ages out.

TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: The number of well-formed TLVs, but with an unknown type value.

Age-Outs: Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed and the Age-Out counter is incremented.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh, Clear): Click “Refresh” to refresh the LLDP Port Statistics information manually or press clear to clean up the entries.

3-9 PoE

Power over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. It could be used to power IP telephones, wireless LAN access points, and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

3-9.1 Configuration

This page allows the user to inspect and configure the current PoE port settings and show all PoE Supply Watts.

Web Interface

To configure Power over Ethernet in the web interface:

1. Click configuration.
2. Specify the Reserved Power determined and Power Management Mode. Specify the PoE or PoE++ and Priority.
3. Click “Apply”.

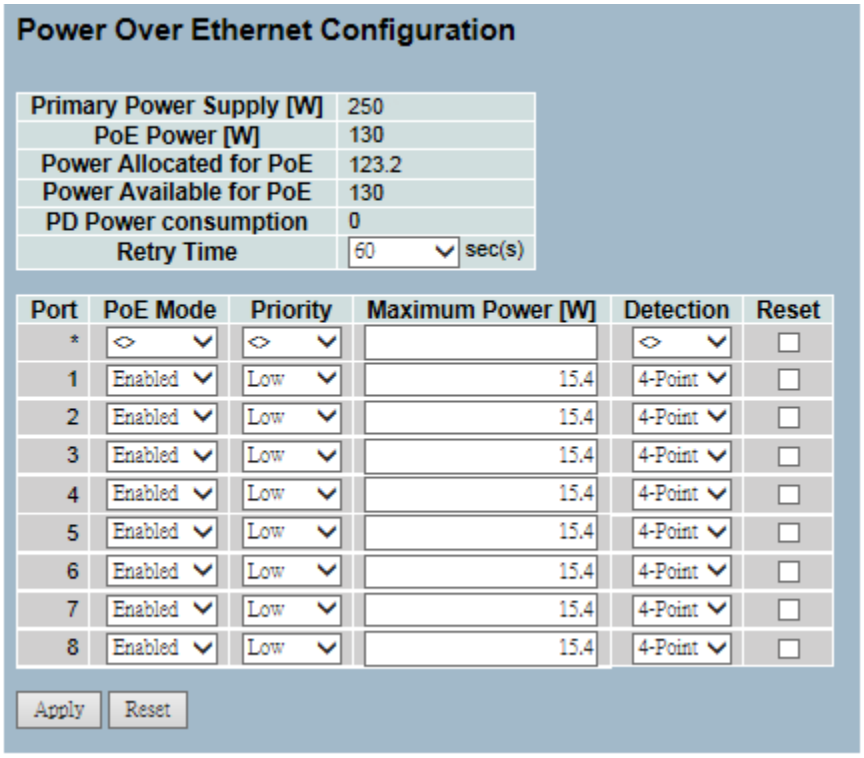

Power Over Ethernet Configuration
Primary Power Supply [W] 250
PoE Power [W] 130
Power Allocated for PoE 123.2
Power Available for PoE 130
PD Power consumption 0
Retry Time 60 sec(s)
Port PoE Mode Priority Maximum Power [W] Detection Reset
* <> <> 15.4
1 Enabled Low 15.4 4-Point
2 Enabled Low 15.4 4-Point
3 Enabled Low 15.4 4-Point
4 Enabled Low 15.4 4-Point
5 Enabled Low 15.4 4-Point
6 Enabled Low 15.4 4-Point
7 Enabled Low 15.4 4-Point
8 Enabled Low 15.4 4-Point
Apply
Reset

Figure 3-9.1: The Power Over Ethernet Configuration

Parameter Description

Power Supply Configuration

Primary Power Supply [W]: The switch can have PoE power supplies. It is used as a power source. To determine the amount of power the PD may use, the amount of power the power sources can deliver must be defined.

PoE Power: The PoE power supply settings will be shown.

Power Allocated for PoE: The total of maximum power.

Power Available for PoE: Power Available for PoE.

PD Power consumption: Shows PD power consumption.

Retry Time: The period (in seconds) for trying to turn on an overloaded PoE port.

1. The retry time function is for per port overload recovery. It is not for over power budget turned off ports recovery.
2. When the PoE switch is over total power budget, the lower priority ports will be turned off immediately.
3. When the over total power budget status changed to the under power budget, the inactive ports will be turned on immediately.

Ethernet Port Configuration

Port: This is the logical port number for this row.

PoE Mode: The PoE Mode represents the PoE operating mode for the port.

- **Disabled:** PoE disabled for the port.
- **Enabled**: Enables PoE IEEE 802.3af/at.

Priority: Priority represents the ports priority. There are three levels of power priority named Low, High, and Critical.

The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case, the port with the lowest priority will be turn off, starting from the port with the highest port number.

Maximum Power: The maximum power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

Detection: Detection represents the PoE capacitor detection for the port.

- **Legacy :** Legacy capacitive detection only.
- **4-point :** IEEE 802.3af 4-point detection only.
- **Both :** IEEE 802.3af 4-point detection followed by legacy detection.

Reset: Resets the specific PoE port.

NOTE: If you want to set the Port support IEEE802.3at, then set the maximum allowed value to 30W.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

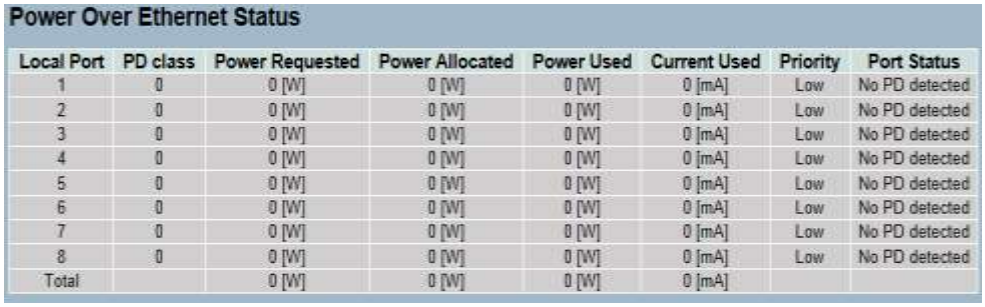
3-9.2 Status

This page allows the user to inspect the current status for all PoE ports. The section shows all Port Power Over Ethernet Status.

Web Interface

To display Power over Ethernet Status in the web interface:

1. Click Status.
2. Display Power Over Ethernet Status Information.
3. Click “Refresh”.



Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Figure 3-9.2: The Power Over Ethernet Status

Parameter Description

Local Port: This is the logical port number for this row.

PD Class: The recognition of PD class generates from the current that PD transmits back to the PSE during the detection between PSE and PD. The current is classified by 802.3 at/af protocol. The PD class shown is a reference. It is not related to the actual PD power requested.

The PD class that the switch read from PD might be inconsistent with the PD specification. There are two reasons that result in this inconsistency.

1. If the PD supports PoE function, the voltage and current of PD design should follow 802.3 af or 802.3 at protocol. If PD design did not fully follow the protocol, the current PD transmitted back to the switch cannot be defined in the classification range that regulated in protocol (in the following table). The switch will define the PD class itself and will be inconsistent.

Classification Category	Classification Current
0 (Type 1)	2.5mA (±2.5mA)
1 (Type 1)	10.5mA (±2.5mA)
2 (Type 1)	18.5mA (±2.5mA)
3 (Type 1)	28mA (±3mA)
4 (Type 2)	40mA (±5mA)

2. When the current is still unstable while PD connect to PSE, and the PD class already has been defined, it may result inconsistency because the PD class is not able to actively adjust. The PD class will adjust after PD unplug and then plug in.

Power Requested: The Power Requested shows the requested amount of power the PD wants to be reserved.

Power Allocated: The Power Allocated shows the amount of power the switch has allocated for the PD.

Power Used: The Power Used shows how much power the PD currently is using.

Current Used: The Power Used shows how much current the PD currently is using.

Priority: The Priority shows the port's priority configured by the user.

Port Status: The Port Status shows the port's status.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the PoE Port information manually.

3-9.3 Power Delay

This section allows the user to set the delay time of power providing after device rebooted.

Web Interface

To display Power over Ethernet Status in the web interface:

1. Click Configuration, PoE, and Power delay.
2. Enable the port to the power device.
3. Specify the power providing delay time when reboot.
4. Click “Apply” to apply the change.

NOTE: There might be a 15 seconds gap between the delay time and actual time. During this gap, the switch implements the action of PD detection by PoE and configuration loading. Meanwhile, the PD process boot up procedure. Different PD may result in different gap on delay time.

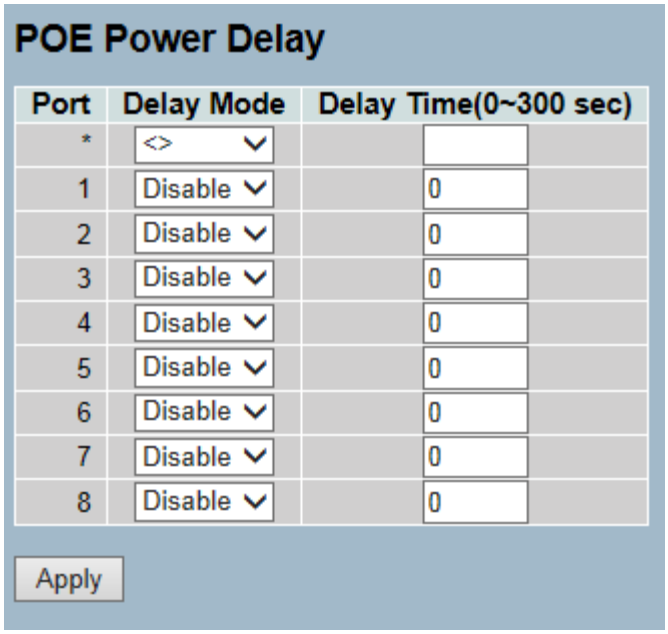


Figure 3-9.3: The POE Power Delay

Parameter Description

Port: This is the logical port number for this row.

Delay Mode: Turn on/off the power delay function.

Delay Time (0~300sec): When rebooting, the PoE port will start to provide power to the PD when it out of delay time.

Button:

- **Apply-** Click “Apply” to apply the change.

3-9.4 Auto Checking

This page specifies the auto detection parameters to check the linking status between PoE ports and PDs. When it detects a fail connection, the remote PD will automatically reboot.

Web Interface

To display Power over Ethernet Auto Checking in the web interface:

1. Click Configuration, PoE, and Auto checking.
2. Enable the Ping Check function.
3. Specify the PD's IP address, checking interval, retry time, failure action, and reboot time.
4. Click "Apply" to apply the change.

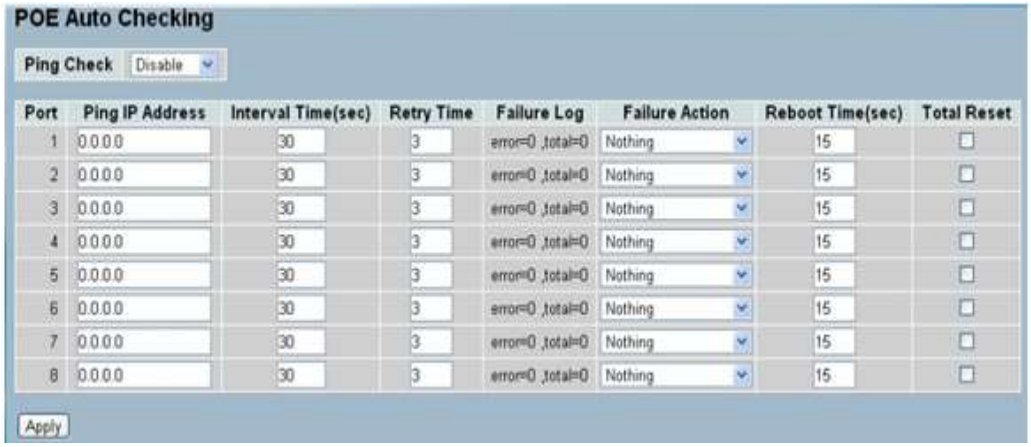

POE Auto Checking
Ping Check
Disable
Port
Ping IP Address
Interval Time(sec)
Retry Time
Failure Log
Failure Action
Reboot Time(sec)
Total Reset
1 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
2 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
3 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
4 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
5 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
6 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
7 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
8 0.0.0.0 30 3 error=0 ,total=0 Nothing 15
Apply

Figure 3-9.4: The POE Auto Checking

CAUTION: When using PoE to power an IP camera or similar device that goes through an initialization period, do not set the "Interval Time" below 20 seconds if the "Failure Action" is set to "Reboot Remote PD". Doing so may prevent the switch from successfully pinging the device and could result in a continuous ON-OFF-ON-OFF cycle of the PoE power.

Parameter Description

Ping Check: Enables the Ping Check function to detect the connection between PoE port and power device. Disable will turn off the detection.

Port: This is the logical port number for this row.

Ping IP Address: The PD's IP Address the system should ping.

Interval Time (sec): Device will send checking message to PD each interval time.

Retry Time: When PoE port is unable to ping the PD, it will retry to send detection again. After the third try, it will trigger failure action.

Failure Log: Failure loggings counter.

Failure Action: The action when the third fail detection.

- **Nothing-** "Nothing" keeps pinging the remote PD but doesn't do any further actions.
- **Reboot Remote PD-** Cuts off the power of the PoE port and forces the PD to reboot.

Reboot time: When PD has been rebooted, the PoE port restores power according to the specified time.

Total Reset: Reset the total value of the "Failure Log".

Button:

- **Apply-** Click "Apply" to apply the change.

3-9.5 Scheduling

This section allows the user to make a perfect schedule of PoE power supply. PoE Scheduling not only makes PoE management easier, but also saves more energy.

Web Interface

To display Power Over Ethernet Scheduling in the web interface:

1. Click Configuration, PoE, and Scheduling.
2. Select the local port and enable.
3. Select time and day for the supply power.
4. Click “Apply” to apply the change.

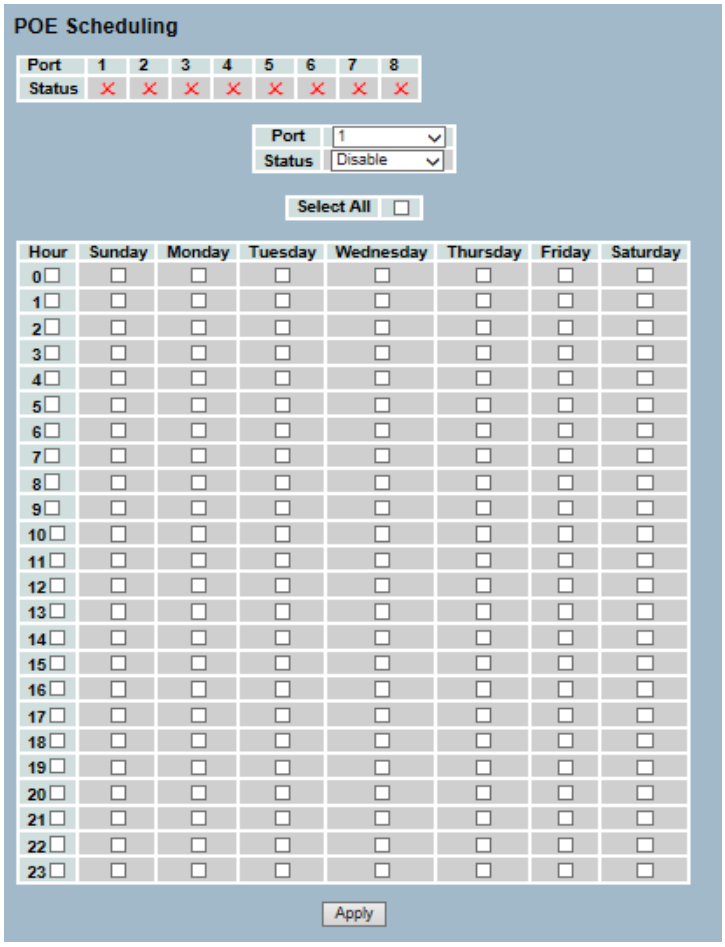

POE Scheduling
Port 1 2 3 4 5 6 7 8
Status
Port 1
Status Disable
Select All
Hour Sunday Monday Tuesday Wednesday Thursday Friday Saturday
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Apply

Figure 3-9.5: The POE Scheduling

Parameter Description

Port / Status: This is the logical port number and its PoE Scheduling mode. ✓ is enable. ✗ is disable.

Week Day (Sun., Mon., …): The days of PoE port provide power of a week.

Hour: The time of PoE port provide power of a day.

Button:

- **Apply-** Click “Apply” to apply the change.

3-10 Filtering Data Base

Filtering Data Base Configuration gathers many functions, including MAC Table Information and Static MAC Learning, which cannot be categorized to some function type.

MAC table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds a table that mapped MAC addresses to switch ports to know which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address). It shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table, if no frame with the corresponding SMAC address has been seen after a configurable age time.

3-10.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic and configure the static MAC table here.

Web Interface

To configure MAC Address Table in the web interface:

Aging Configuration

1. Click configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click “Apply”.

MAC Table Learning

1. Click configuration.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click “Apply”.

Static MAC Table Configuration

1. Click configuration and add new static entry .
2. Specify the VLAN IP and Mac address, Port Members.
3. Click “Apply”.

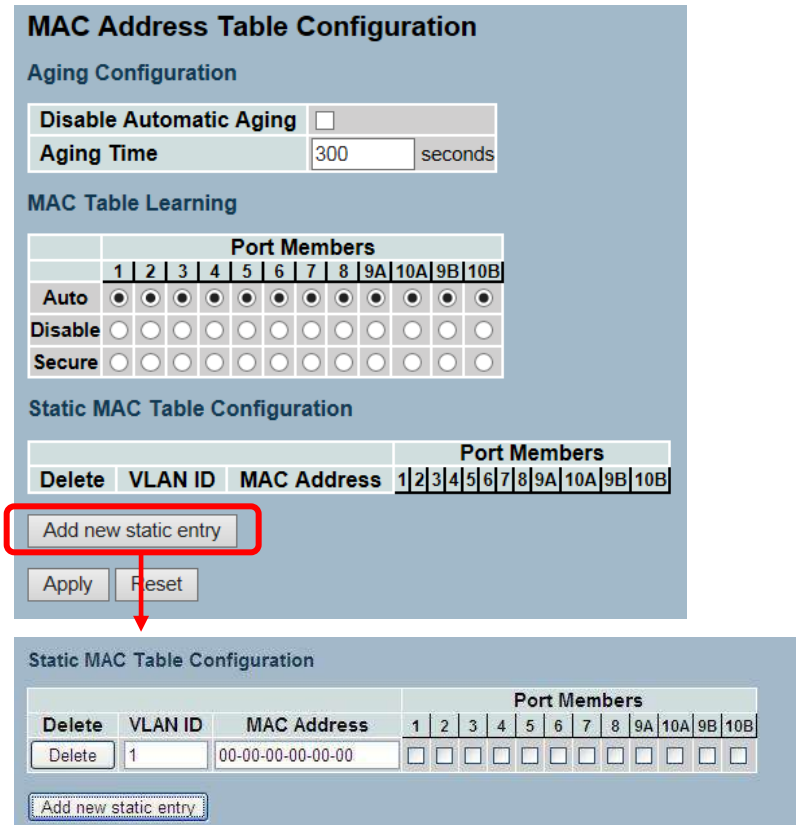


Figure 3-10.1: The MAC Address Table Configuration

Parameter Description

Aging Configuration: By default, the dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging. Configure aging time by entering a value in seconds. For example, age time seconds. The allowed range is 10 to 1000000 seconds. Disables the automatic aging of dynamic entries by checking

☑ Disable Automatic Aging.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode and cannot be changed by the user. An example of such module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

- **Auto:** Learning is done automatically, as soon as a frame with unknown SMAC is received.
- **Disable:** No learning is done.
- **Secure:** Only static MAC entries are learned, all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode. Otherwise, the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete: Check to delete the entry. It will be deleted during the next save.

VLAN ID: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry: Click to add a new entry to the static MAC table. Specifies the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-10.2 Dynamic MAC Table

Entries in the MAC table are shown on this page. The MAC table contains up to 8192 entries. It is sorted first by VLAN ID, and then by MAC address.

Web Interface

To display MAC Address Table in the web interface:

1. Click Dynamic MAC Table.
2. Specify the VLAN and MAC Address.
3. Display MAC Address Table.

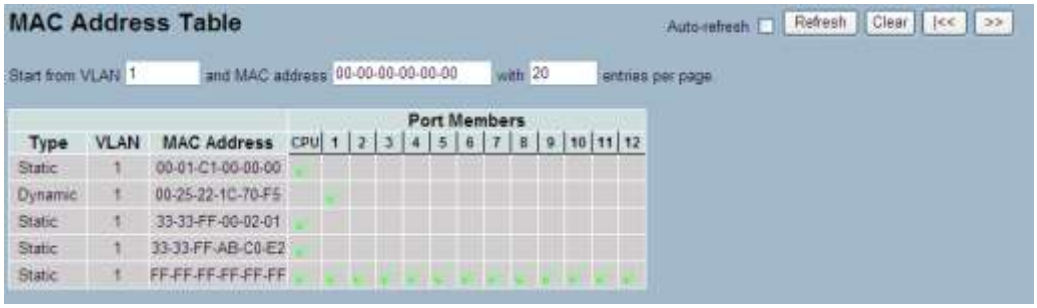


Figure 3-10.2: The Dynamic MAC Address Table information

Parameter Description

MAC Table Columns

Switch (stack only) - The stack unit where the entry is learned.

Type: Indicates whether the entry is a static or a dynamic entry.

VLAN: The VLAN ID of the entry.

MAC address: The MAC address of the entry.

Port Members: The ports that are members of the entry.

Auto-refresh: Evoke the auto-refresh icon, then the device will refresh the information automatically.

Upper right icon (Refresh, Clear, <<, >>): Click “Refresh” to refresh the MAC address entries manually or press clear to clean up the MAC table. Press **<<** or **>>** to go up or down a page of the table.

3-11 VLAN

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1. However, you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN, or connect to the new management VLAN through a multi-VLAN route.

3-11.1 VLAN Membership

The VLAN membership configuration for the selected stack switch and unit switch can be monitored and modified here. Up to 4096 VLANs are supported. The user is allowed to add and delete VLANs, and port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN membership Configuration.
2. Specify Management VLAN ID from 0 to 4094.
3. Click “Apply”.

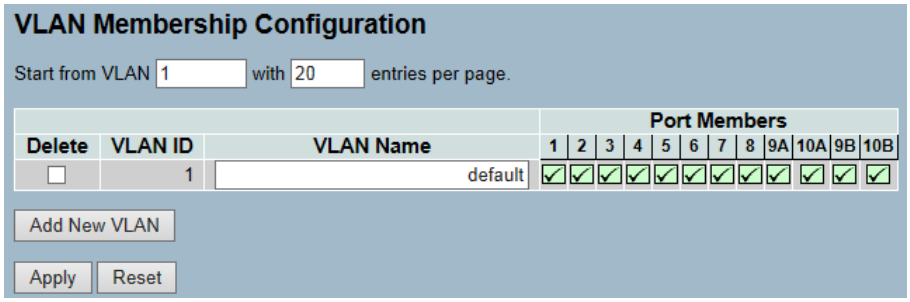


Figure 3-11.1: The VLAN Membership Configuration

Parameter Description

Delete: To delete a VLAN entry, check this box. The entry will be deleted on the selected switch in the stack. If none of the ports of this switch are members of a VLAN, then the delete checkbox will be greyed out. That entry cannot be deleted.

VLAN ID: Indicates the ID of this particular VLAN.

VLAN Name: Indicates the name of VLAN. VLAN Name can only contain alphabets or numbers. VLAN name should contain at least one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

Port Members: A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New VLAN: Click to add a new VLAN ID. An empty row is added to the table and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is, thereafter, presented on the other stack switch units but with no port members. The check box is greyed out when VLAN is displayed on other stacked switches, but user can add member ports to it.

A VLAN, without any port members on any stack unit, will be deleted when you click "Save".

The button can be used to undo the addition of new VLANs.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-11.2 Ports

As a function in VLAN Tag Rule Setting, the user can input VID number to each port. The range of VID number is from 1 to 4094. The user also can choose ingress filtering rules for each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is to forward only packets with VID matching this port's configured VID. The Ingress Filtering Rule 2 is to drop untagged frame. You can also select the role of each port as Access, Trunk, or Hybrid.

Web Interface

To configure VLAN Port configuration in the web interface:

1. Click VLAN Ports.
2. Specify the VLAN Port Configuration parameters.
3. Click "Apply".

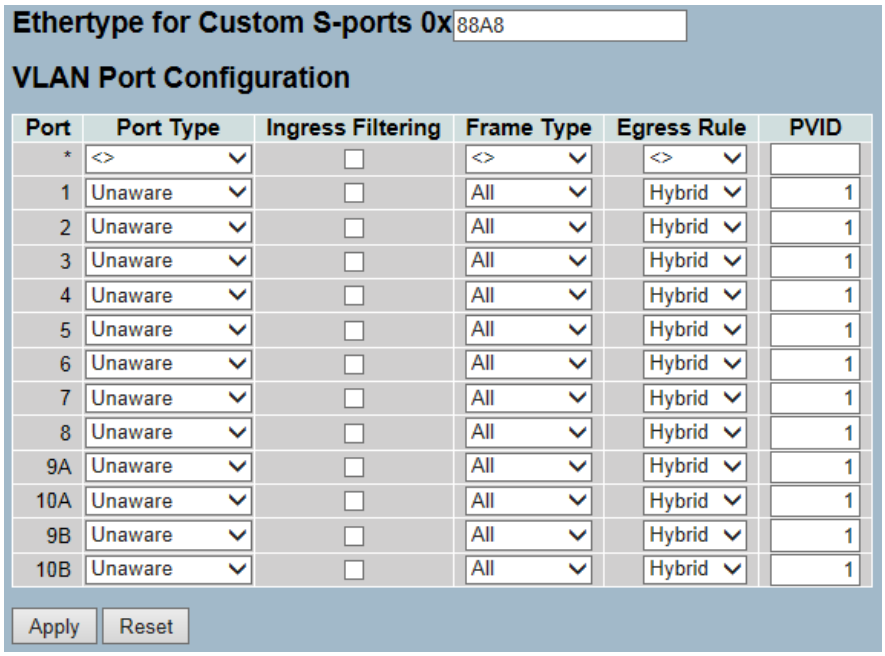


Figure 3-11.2: The VLAN Port Configuration

Parameter Description

Ethertype for Custom S-ports: This field specifies the Ethertype used for custom S-ports. This is a global setting for all the custom S-ports. Custom Ethertype lets the user change the Ethertype value on a port to any value. This supports network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 802.1p-tagged frames.

Port: This is the logical port number of this row.

Port Type: Port can be one of the following types: Unaware, Customer port (C-port), Service port (S-port), or Custom Service port (S-custom-port).

If the port type is unaware, all frames are classified to the Port VLAN ID and tags are not removed.

Ingress Filtering: Enables ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

Frame Type: Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to all.

Egress Rule: Determines which device the port connects to. If the port connects to VLAN-unaware devices, the access link should be used (e.g. terminal/work station). If the port connect to VLAN-aware devices, the trunk link should be used (e.g. switch connect to switch). Hybrid link is used for more flexible application.

- **Hybrid**: If the tag of tagged frame is as the same as PVID, the tag of the frame will be removed. The frame become an untagged frame and transmitted.
- Any other tagged frame whose tag value is different from PVID is transmitted directly.
- **Trunk**: All tagged frames with any tag value are transmitted.
- **Access**: The tag of any tagged frame will be removed to become an untagged frame. These untagged frames will be transmitted.

Port VLAN ID: Configures the VLAN identifier for the port. The allowed values are 1 through 4094. The default value is 1.

NOTE: The port must be a member of the same VLAN as the Port VLAN ID.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-11.3 Switch Status

The function of the switch status is to gather all information about the VLAN status and report it by the order of static – NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.

Web Interface

To display VLAN membership status in the web interface:

1. Click VLAN membership.
2. Specify the Static – NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP Combined.
3. Display membership information.

Figure 3-11.3: The VLAN Membership Status for Static User

Parameter Description

VLAN USER (You can scroll to select one kind VLAN user as below :)

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations, such as PVID and UVID. Currently, we support the following VLAN user types:

- **CLI/Web/SNMP:** These are referred to as static.
- **NAS:** NAS provides port-based authentication, which involves communications between a Supplicant, an Authenticator, and an Authentication Server.
- **MVRP:** Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.
- **GVRP:** GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.
- **Voice VLAN:** Voice VLAN is a VLAN configured specifically for voice traffic typically originating from IP phones.
- **MVR:** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
- **MSTP:** The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.
- **Port Members:** A row of check boxes for each port is displayed for each VLAN ID.
  If a port is included in a VLAN, an image ✓ will be displayed.
  If a port is included in a Forbidden port list, an image ✗ will be displayed.
  If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✗.

VLAN Membership: The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When all VLAN Users are selected, it shows this

information for all the VLAN Users. This is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the VLAN entries manually.

3-11.4 Port Status

The function of the port status is to gather all information about the VLAN status and reports it by the order of static – NAS, MVRP, MVP, Voice VLAN, MSTP, and GVRP Combined.

Web Interface

To display VLAN Port Status n the web interface:

1. Click VLAN port status.
2. Specify the static – NAS, MVRP, MVP, Voice VLAN, MSTP, or GVRP Combined.
3. Display port status information.

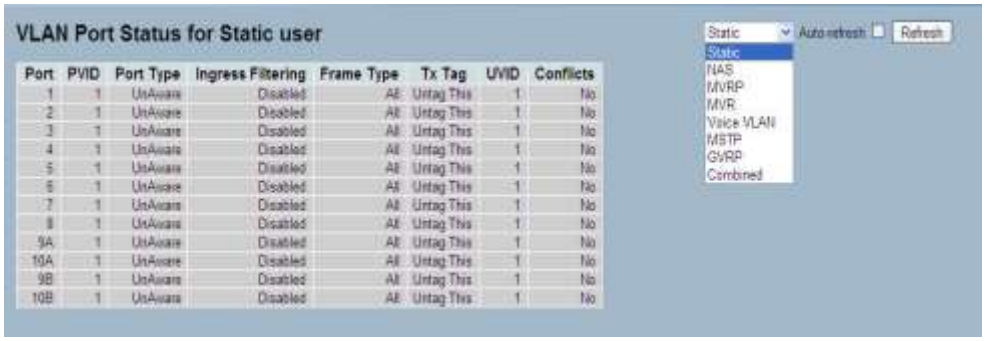

VLAN Port Status for Static user
Static
Auto-refresh
Refresh
Static
NAS
MVRP
MVR
Voice VLAN
MSTP
GVRP
Combined
Port PVID Port Type Ingress Filtering Frame Type Tx Tag UVID Conflicts
1 1 UnAware Disabled All Untag This 1 No
2 1 UnAware Disabled All Untag This 1 No
3 1 UnAware Disabled All Untag This 1 No
4 1 UnAware Disabled All Untag This 1 No
5 1 UnAware Disabled All Untag This 1 No
6 1 UnAware Disabled All Untag This 1 No
7 1 UnAware Disabled All Untag This 1 No
8 1 UnAware Disabled All Untag This 1 No
9A 1 UnAware Disabled All Untag This 1 No
10A 1 UnAware Disabled All Untag This 1 No
9B 1 UnAware Disabled All Untag This 1 No
10B 1 UnAware Disabled All Untag This 1 No

Figure 3-11.4: The VLAN Port Status for Static user

Parameter Description

Port: The logical port for the settings contained in the same row.

PVID: Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.

Port Type: Shows the Port Type. Port type can be any of the following - Unaware, C-port, S-port, or Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

Ingress Filtering: Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If the ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type: Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Tx Tag: Shows egress filtering frame status whether tagged or untagged.

UVID: Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

Conflicts: Shows whether the status of conflicts exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional Conflicts between features.
- Conflicts due to hardware limitation.

- Direct conflict between user modules.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the VLAN Port Status information manually.

3-11.5 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

3-11.5.1 Private VLANs Membership

The private VLAN membership configurations for the switch can be monitored and modified. Private VLANs can be added or deleted. Port members of each private VLAN can be added or removed. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure Private VLAN configuration in the web interface:

1. Click add new Private VLAN Membership.
2. Specify the Private VLAN ID and Port Members.
3. Click “Apply”.

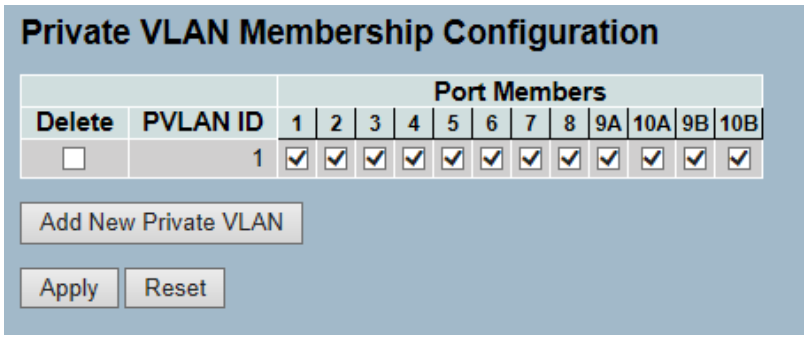


Figure 3-11.5.1: The Private VLAN Membership Configuration

Parameter Description

Delete: To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID: Indicates the ID of this particular private VLAN.

Port Members: A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Private VLAN: Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-11.5.2 Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises of a switch that has plurality of ports. Each port is configured as a protected port or a non-protected port. An address table memory stores an address table that has a destination address and port number pair. A forwarding map generator creates a forwarding map, which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch is to configure each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on the layer 2 switch. A forwarding map is generated for the data packet based upon the destination address on the data packet. Then the data packet is sent to the plurality of ports pursuant to the forwarding map generated, based upon whether the ingress port was configured as a protected or non-protected port.

This page is used to enable or disable port isolation on ports in a private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN, Port Isolation.
2. Evoke which port want to enable Port Isolation.
3. Click “Apply”.

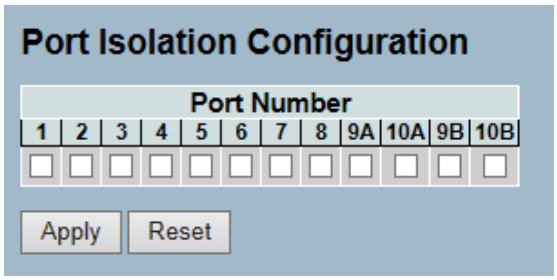


Figure 3-11.5.2: The Port Isolation Configuration

Parameter Description

Port Members: A check box is provided for each port of a private VLAN. When checked, the port isolation is enabled on that port. When unchecked, the port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-11.6 MAC-Based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame, based on the source MAC address of the frame.

A most common way of grouping the VLAN members is by port, hence the name "Port-Based VLAN". Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. Meanwhile, to provide user access and ensure data security, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

3-11.6.1 Configuration

The MAC-based VLAN entries can be configured here. Mac-based VLAN entries can be added or deleted. Entries can also be assigned to different ports. This section only shows static entries.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click MAC address-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click "Apply".

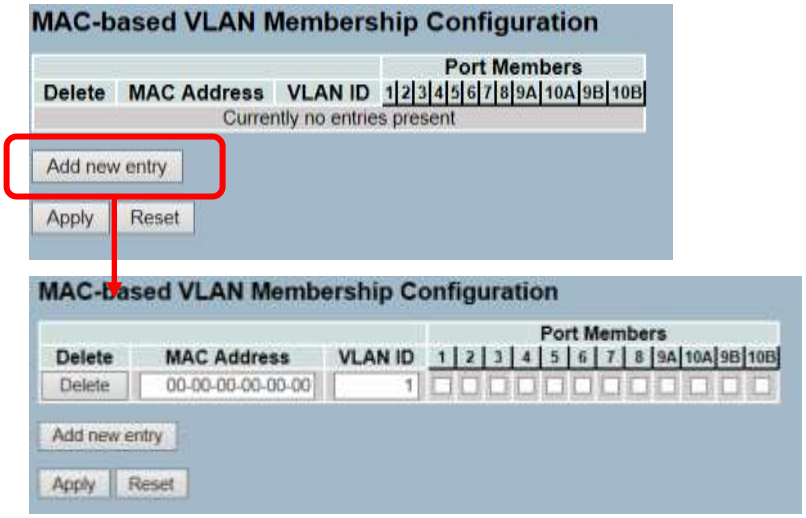


Figure 3-11.6.1: The MAC-based VLAN Membership Configuration

Parameter Description

Delete: To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

MAC Address: Indicates the MAC address.

VLAN ID: Indicates the VLAN ID.

Port Members: A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New MAC-based VLAN: Click to add a new MAC-based VLAN entry. An empty row is added to the table and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 to 4095.

The MAC-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save".

The button can be used to undo the addition of new MAC-based VLANs.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-11.6.2 Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently, we support the following VLAN user types:

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, an Authenticator, and an Authentication Server.

Web Interface

To display MAC-based VLAN configured in the web interface:

1. Click MAC-based VLAN Status.
2. Specify the Static NAS Combined.
3. Display MAC-based information.

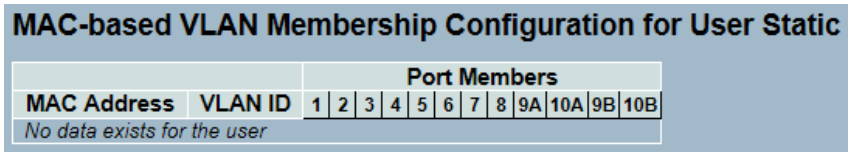

MAC-based VLAN Membership Configuration for User Static
Port Members
MAC Address
VLAN ID
1 2 3 4 5 6 7 8 9A 10A 9B 10B
No data exists for the user

Figure 3-11.6.2: The MAC-based VLAN Membership Status for User Static

Parameter Description

MAC Address: Indicates the MAC address.

VLAN ID: Indicates the VLAN ID.

Port Members: Port members of the MAC-based VLAN entry.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the MAC-based VLAN Membership information manually.

3-11.7 Protocol-Based VLAN

Protocol-based VLAN is described in details in this section. The switch supports Protocol and Ethernet LLC SNAP Protocol.

LLC: The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is layer 2; just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet, and Appletalk) to coexist within a multipoint network and be transported over the same network media. It can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP: The Subnet work Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC. More protocols can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values. It also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11, and other IEEE 802 physical network layers, as well as, with non-IEEE 802 physical network layers (e.g. FDDI that use 802.2 LLC).

3-11.7.1 Protocol to Group

The user can add new protocols to Group Name (unique for each Group) to map entries. The user can also view and delete already mapped entries for the selected stack switch unit switch.

Web Interface

To configure Protocol-based VLAN configuration in the web interface:

1. Click Protocol-based VLAN protocol to group and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click “Apply”.

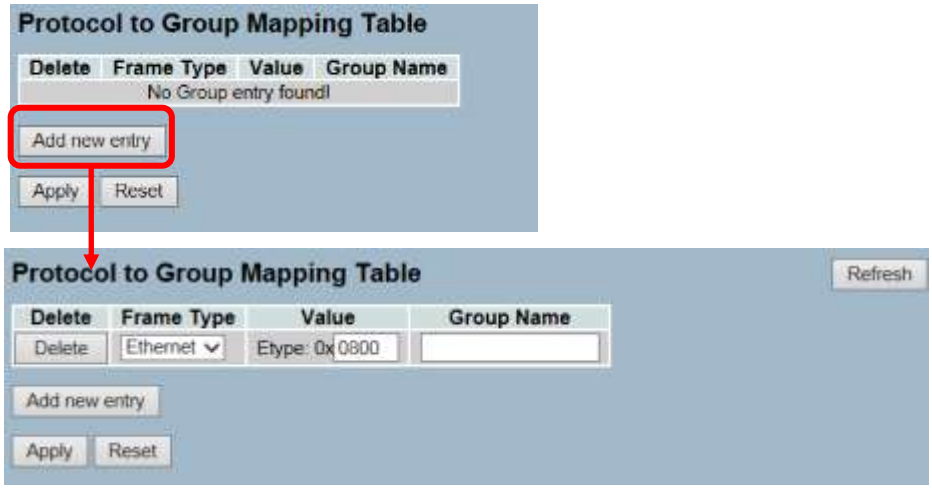


Figure 3-11.7.1: The Protocol to Group Mapping Table

Parameter Description

Delete: To delete a protocol from Group Name map entry, check this box. The entry will be deleted on the switch during the next save.

Frame Type: Frame Type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

NOTE: On changing the frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

Value: Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria's for three different frame types:

1. **For Ethernet:** Values in the text field when Ethernet is selected as a frame type is called etype. Valid values for etype ranges from 0x0600-0xfff0.
2. **For LLC:** Valid value in this case is comprised of two different sub-values.
    a. **DSAP**: 1-byte long string (0x00-0xff)
    b. **SSAP**: 1-byte long string (0x00-0xff)
3. **For SNAP:** Valid value in this case also is comprised of two different sub-values.
    a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx, where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
    b. **PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
    In other words, if the value of OUI field is 00-00-00, then the value of PID will be etype (0x0600-0xffff). If the value of OUI is other than 00-00-00, then the valid value of PID will be any value from 0x0000 to 0xffff.

Group Name: A valid group name is a unique 16-character long string for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

NOTE: Special character and underscore (_) are not allowed.

Adding a New Group to VLAN mapping entry: Click to add a new entry in the mapping table. An empty row is added to the table. Frame Type, value, and the group name can be configured as needed.

The button can be used to undo the addition of new entry.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh): Click “Refresh” to refresh the Protocol Group Mapping information manually.

3-11.7.2 Group to VLAN

The user can map an already configured Group Name to a VLAN for the selected stack unit switch.

Web Interface

To display Group Name to VLAN mapping table configured in the web interface:

1. Click Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click “Apply”.

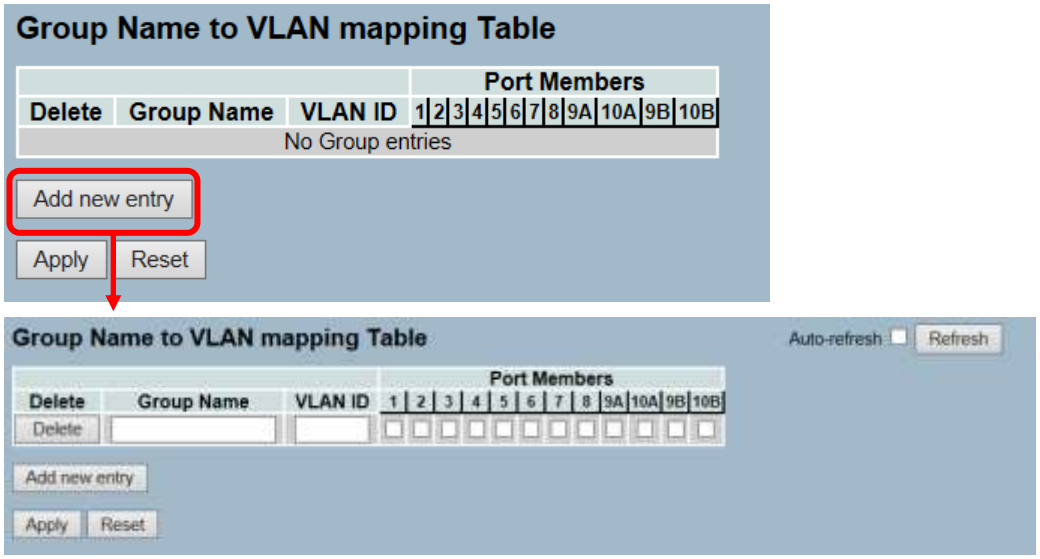


Figure 3-11.7.2: The Group Name of VLAN Mapping Table

Parameter Description

Delete: To delete a group name to VLAN map entry, check this box. The entry will be deleted on the switch during the next save.

Group Name: A valid Group Name is a string of at most 16 characters, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). No special character is allowed. The group name you’re trying to map to a VLAN must be present in Protocol to Group mapping table and must not be previously used by any other existing mapping entry on this page.

VLAN ID: Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

Port Members: A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New Group to VLAN mapping entry: Click to add a new entry in mapping table. An empty row is added to the table, Group Name, VLAN ID, and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the Protocol Group Mapping information manually.

3-12 Voice VLAN

Voice VLAN is VLAN configured specifically for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data to ensure the transmission priority of voice traffic and voice quality.

3-12.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there are two VLANs on a port - one for voice and one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

1. Select “Enabled” in the Voice VLAN Configuration.
2. Specify VLAN ID Aging Time Traffic Class.
3. Specify (Port Mode, Security, and Discovery Protocol) in the Port Configuration.
4. Click “Apply”.

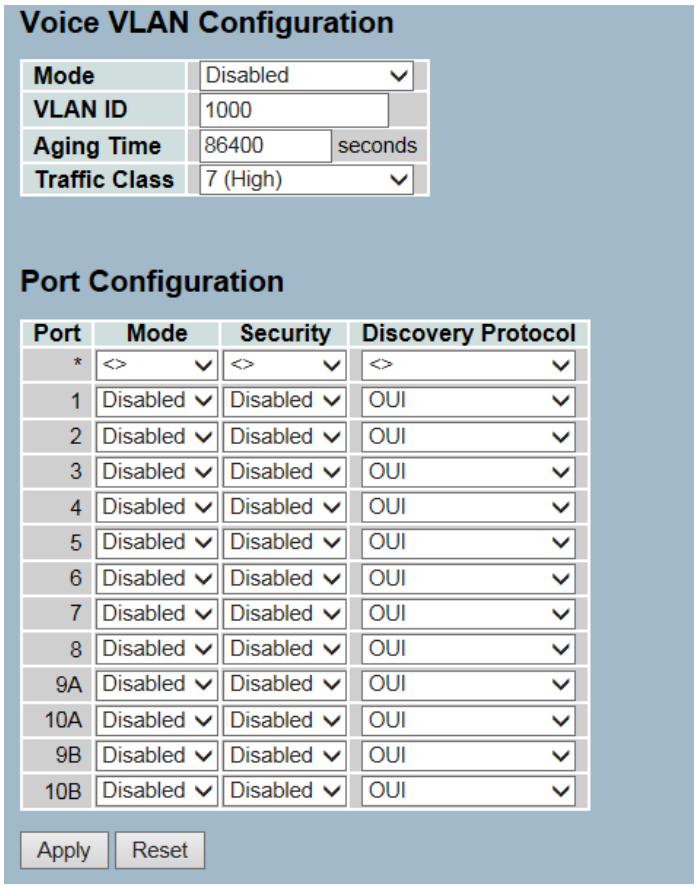


Figure 3-12.1: The Voice VLAN Configuration

Parameter Description

Mode: Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

- **Enabled:** Enables Voice VLAN mode operation.
- **Disabled:** Disables Voice VLAN mode operation.

VLAN ID: Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID, etc. The allowed range is 1 to 4095.

Aging Time: Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode: Indicates the Voice VLAN port mode.

When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.

Possible port modes are:

- **Disabled:** Disjoins from Voice VLAN.
- **Auto:** Enables auto detect mode. It detects whether there is a VoIP phone attached to the specific port and configures the Voice VLAN members automatically.
- **Forced:** Forces join to Voice VLAN.

Port Security: Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

- **Enabled:** Enables Voice VLAN security mode operation.
- **Disabled:** Disables Voice VLAN security mode operation.

Port Discovery Protocol: Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart the auto detect process. Possible discovery protocols are:

- **OUI:** Detects telephony device by OUI address.
- **LLDP:** Detects telephony device by LLDP.
- **Both:** Both OUI and LLDP.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-12.2 OUI

The section describes how to configure the VOICE VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of the OUI process.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Select “Add new entry”, ”Delete” in the Voice VLAN OUI table.
2. Specify Telephony OUI, Description.
3. Click “Apply”.

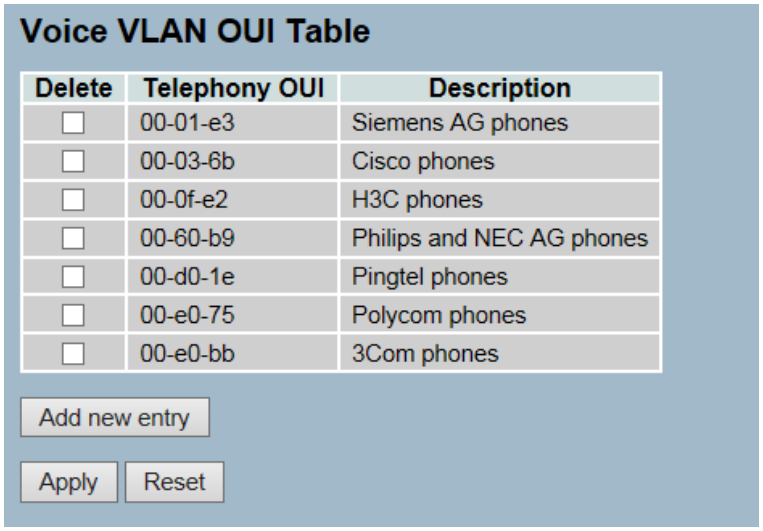


Figure 3-12.2: The Voice VLAN OUI Table

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Telephony OUI: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description: The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Add New entry: Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the Telephony OUI, Description.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-13 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework, whereby devices in a bridged LAN (e.g. end stations and switches) can register and de-register attribute values (e.g. VLAN Identifiers) with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

3-13.1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure GARP Port Configuration in the web interface:

1. Click GARP configure.
2. Specify GARP Configuration Parameters.
3. Click “Apply”.

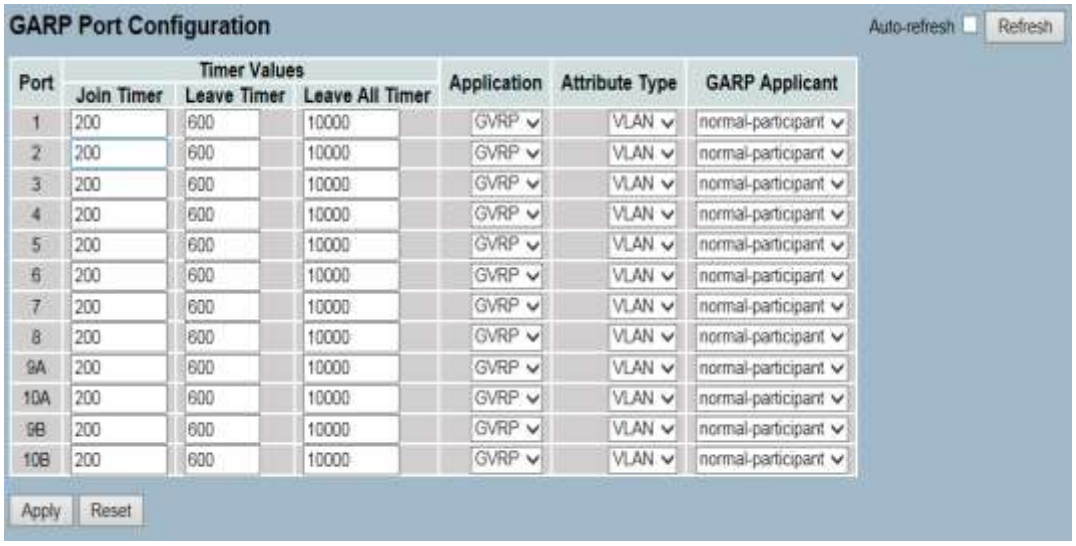

GARP Port Configuration
Auto-refresh
Refresh
Port
Timer Values
Join Timer
Leave Timer
Leave All Timer
Application
Attribute Type
GARP Applicant
1 200 600 10000 GVRP VLAN normal-participant
2 200 600 10000 GVRP VLAN normal-participant
3 200 600 10000 GVRP VLAN normal-participant
4 200 600 10000 GVRP VLAN normal-participant
5 200 600 10000 GVRP VLAN normal-participant
6 200 600 10000 GVRP VLAN normal-participant
7 200 600 10000 GVRP VLAN normal-participant
8 200 600 10000 GVRP VLAN normal-participant
9A 200 600 10000 GVRP VLAN normal-participant
10A 200 600 10000 GVRP VLAN normal-participant
9B 200 600 10000 GVRP VLAN normal-participant
10B 200 600 10000 GVRP VLAN normal-participant
Apply
Reset

Figure 3-13.1: The GARP Port Configuration

Parameter Description

Port: The port column shows the list of ports for which you can configure GARP settings. There are 2 types of configuration settings that can be configured on per port bases.

- Timer Values
- Application
- Attribute Type
- GARP Applicant

Timer Values: To set the GARP - join timer, leave timer, and leave all timers. The unit is micro-second. Three different timers can be configured on this page:

- **Join Timer:** The default value for “Join Timer” is 200ms.
- **Leave Timer:** The range of values for “Leave Timer” is 600-1000ms. The default value for “Leave Timer” is 600ms.
- **Leave All Timer:** The default value for “Leave All Timer” is 10000ms.
- **Application:** Currently, the only supported application is GVRP.

Attribute Type: Currently, the only supported Attribute Type is VLAN.

GARP Applicant: This configuration is used to configure the applicant state machine behavior for GARP on a particular port locally.

- **Normal-participant:** In this mode, the applicant state machine will operate normally in GARP protocol exchanges.
- **Non-participant:** In this mode, the applicant state machine will not participate in the protocol operation.
- The default configuration is normal participant.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-13.2 Statistics

The port statistics of GARP for all switch ports are described in details in this section. The port statistics are related to the currently selected stack units, as reflected by the page header.

Web Interface

To display GARP Port statistics in the web interface:

1. Click GARP statistics.
2. Scroll which port you want to display the GARP counter information.
3. Click Refresh to modify the GARP statistics information.

Figure 3-13.2: The GARP Port Statistics

Parameter Description

Port: The port column shows the list of all ports, for which per port GARP statistics are shown.

Peer MAC: Peer MAC is the MAC address of the neighbor switch from with GARP frame is received.

Failed Count: Explains failed count here.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the GARP Port Statistics information manually.

3-14 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP). It is mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function to provide the VLAN registration service through a GARP application. It makes use of the GARP Information Declaration (GID) to maintain ports associated with their attribute database and GARP Information Propagation (GIP) in order to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintains the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

3-14.1 Configuration

This page allows you to configure the basic GVRP configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure GVRP Port Configuration in the web interface:

1. Click GVRP configure.
2. Specify GVRP Configuration Parameters.
3. Click “Apply”.

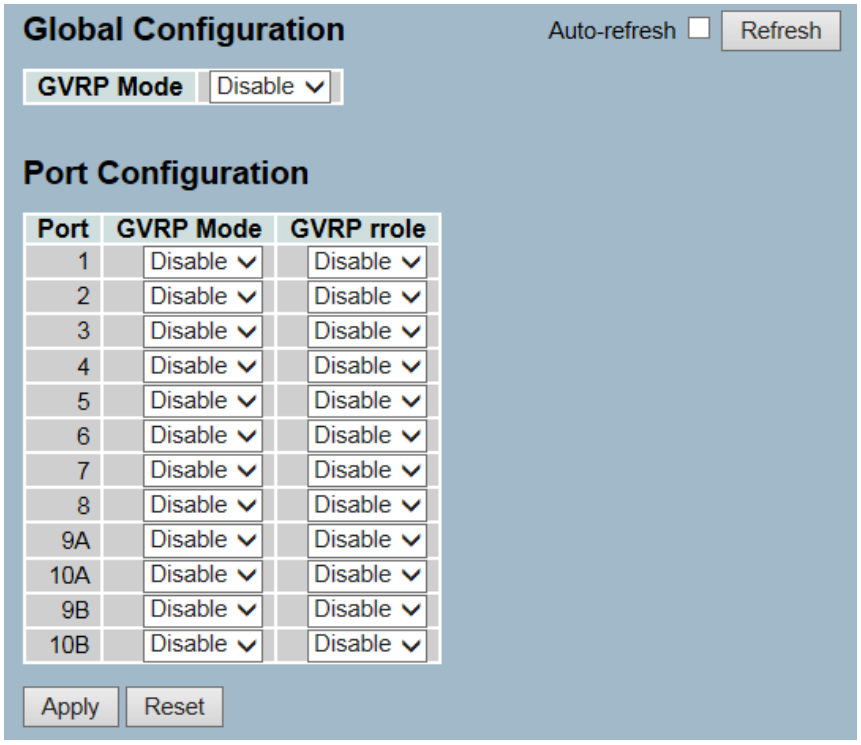


Figure 3-14.1: The GVRP Global Configuration

Parameter Description

GVRP Mode: GVRP Mode is a global setting. To enable the GVRP globally, select "Enable" from menu. To disable GVRP globally, select "Disable". In stacking, this configuration command sends a message to all the slaves connected in stack.

The default value of Global MVRP Mode is "Disable".

Port: The port column shows a list of ports that could be configure per port GVRP settings. There are three configuration settings that can be configured on a per port bases.

1. GVRP Mode: This configuration is to enable/disable GVRP Mode on a particular port locally.

- **Disable:** Select to disable GVRP mode on this port.
- **Enable:** Select to enable GVRP mode on this port.

The default value of configuration is disable.

2. GVRP rrole: This configuration is used to configure restricted role on an interface.

- **Disable:** Select to disable GVRP rrole on this port.
- **Enable:** Select to enable GVRP rrole on this port.

The default configuration is disable.

Auto-refresh: Check "Auto-Refresh" so the device can refresh the information automatically.

Upper right icon (Refresh): Click "Refresh" to refresh the GVRP Global configuration information manually.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset-** Click "Reset" to undo any changes made locally and revert to previously saved values.

3-14.2 Statistics

The section shows the basic GVRP port statistics for all switch ports. The statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display GVRP Port statistics in the web interface:

1. Click GVRP statistics.
2. Scroll which port you want to display the GVRP Counter information.
3. Click Refresh to modify the GVRP statistics information.

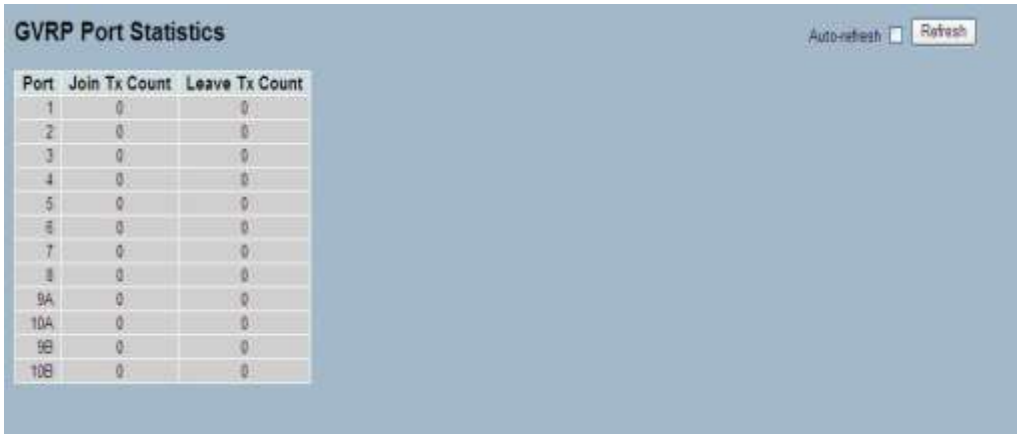


Figure 3-14.2: The GVRP Port Statistics

Parameter Description

Port: The port column shows the list of ports for which you can see port counters and statistics.

Join Tx Count: Explains Join Tx Count here.

Leave Tx Count: Explains Leave Tx Count here.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the GVRP Port Statistics information manually.

3-15 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device to provide queuing, scheduling, and congestion control guarantees to the frame, according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms to provide excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU, even when all the QoS class queues are congested.

3-15.1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports and the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, Port Classification.
2. Scroll to select QoS class, DP Level, PCP and DEI parameters.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

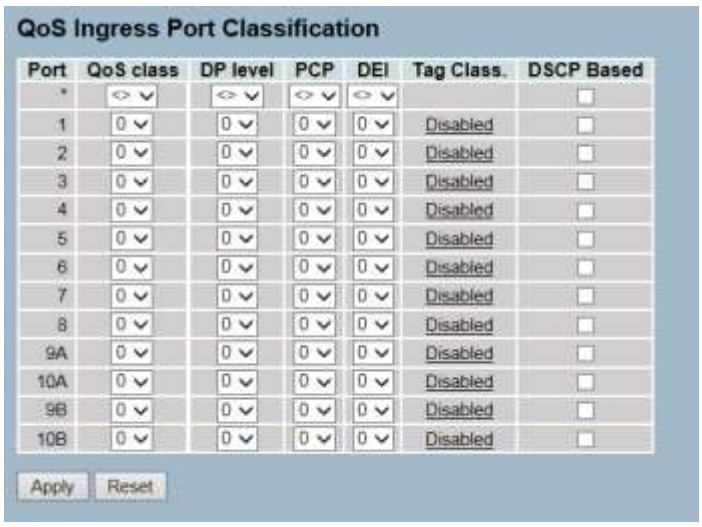


Figure 3-15.1: The QoS Configuration

Parameter Description

Port: The port number for which the configuration below applies.

QoS class: Controls the default QoS class (e.g. the QoS class for frames not classified in any other way). There is a one-to-one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.

DP level: Controls the default DP level (e.g. the DP level for frames not classified in any other way).

PCP: Controls the default PCP for untagged frames.

DEI: Controls the default DEI for untagged frames.

Tag Class.: Shows the classification mode for tagged frames on this port.

- **Disabled:** Uses the default QoS class and DP level for tagged frames.
- **Enabled:** Uses the mapped versions of PCP and DEI for tagged frames.
- Click on the mode in order to configure the mode and/or mapping.

DSCP Based: Click to enable DSCP Based QoS Ingress Port Classification.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.2 Port Policing

This section provides an overview of the QoS Ingress Port Policers for all switch ports. The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Policing.
2. Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll to select the Rate limit Unit with Kbps, Mbps, Fps and Kfps.
4. Click “Apply” to save the configuration.

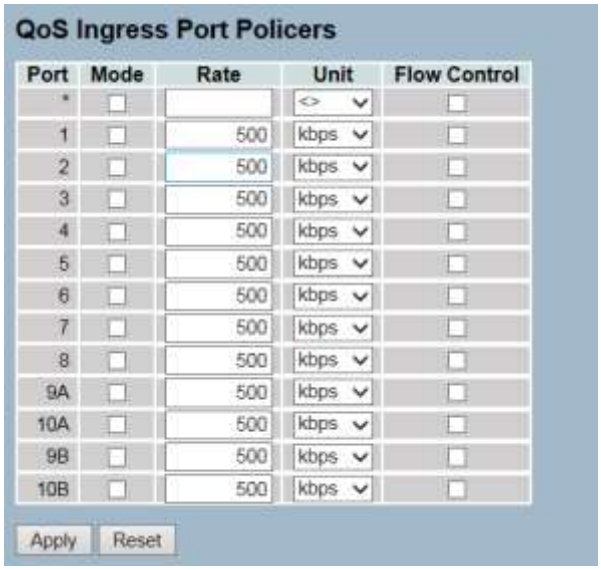


Figure 3-15.2: The QoS Ingress Port Policers Configuration

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode: Controls whether the policer is enabled on this switch port.

Rate: To set the rate limit value for this port. The default is 500.

Unit: To scroll to select what unit of rate includes Kbps, Mbps, Fps, and Kfps. The default is Kbps.

Flow Control: If the flow control is enabled and the port is in flow control mode, then the pause frames are sent instead of discarding frames.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.3 Port Schedulers

This section provides an overview of QoS Egress Port Schedulers for all switch ports and the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

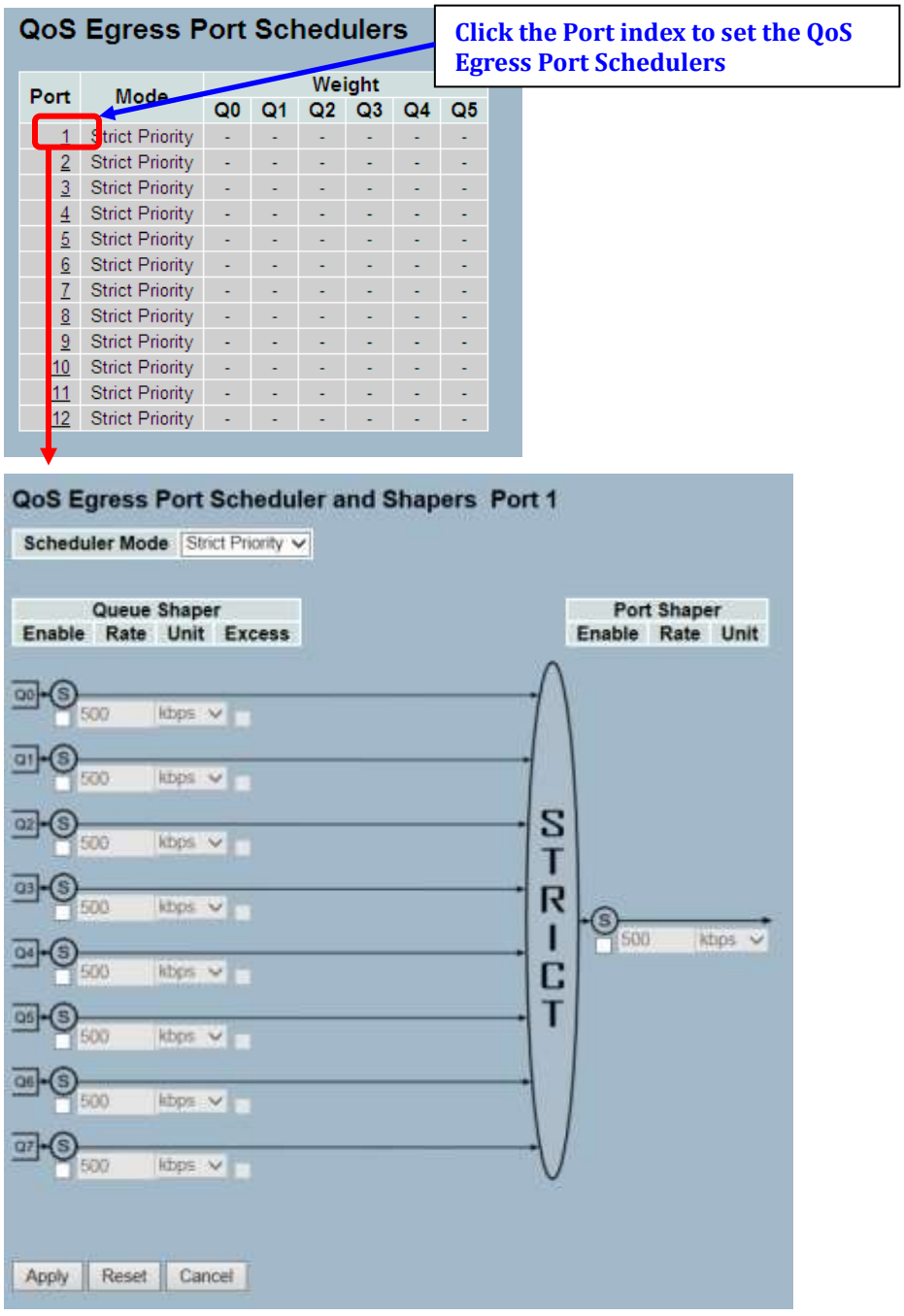


Figure 3-15.3: The QoS Egress Port Schedules

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode: Shows the scheduling mode for this port.

Weight (Qn): Shows the weight for this queue and port.

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. The default value is “?”. This value is restricted to?-1000000, when the "Unit" is "Kbps". It is restricted to 1-?, when the "Unit" is "Mbps”.

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "Kbps" or "Mbps". The default value is "Kbps".

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. The default value is “?”. This value is restricted to?-1000000, when the "Unit" is "Kbps". It is restricted to 1-?, when the "Unit" is "Mbps".

Port Shaper Unit: Controls the unit of measure for the port shaper rate as "Kbps" or "Mbps". The default value is "Kbps".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.4 Port Shaping

This section provides an overview of QoS Egress Port Shapers for all switch ports. The user could also get all detail information to the ports that belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Shapers in the web interface:

1. Click Configuration, QoS, Port Shapers.
2. Display the QoS Egress Port Shapers.

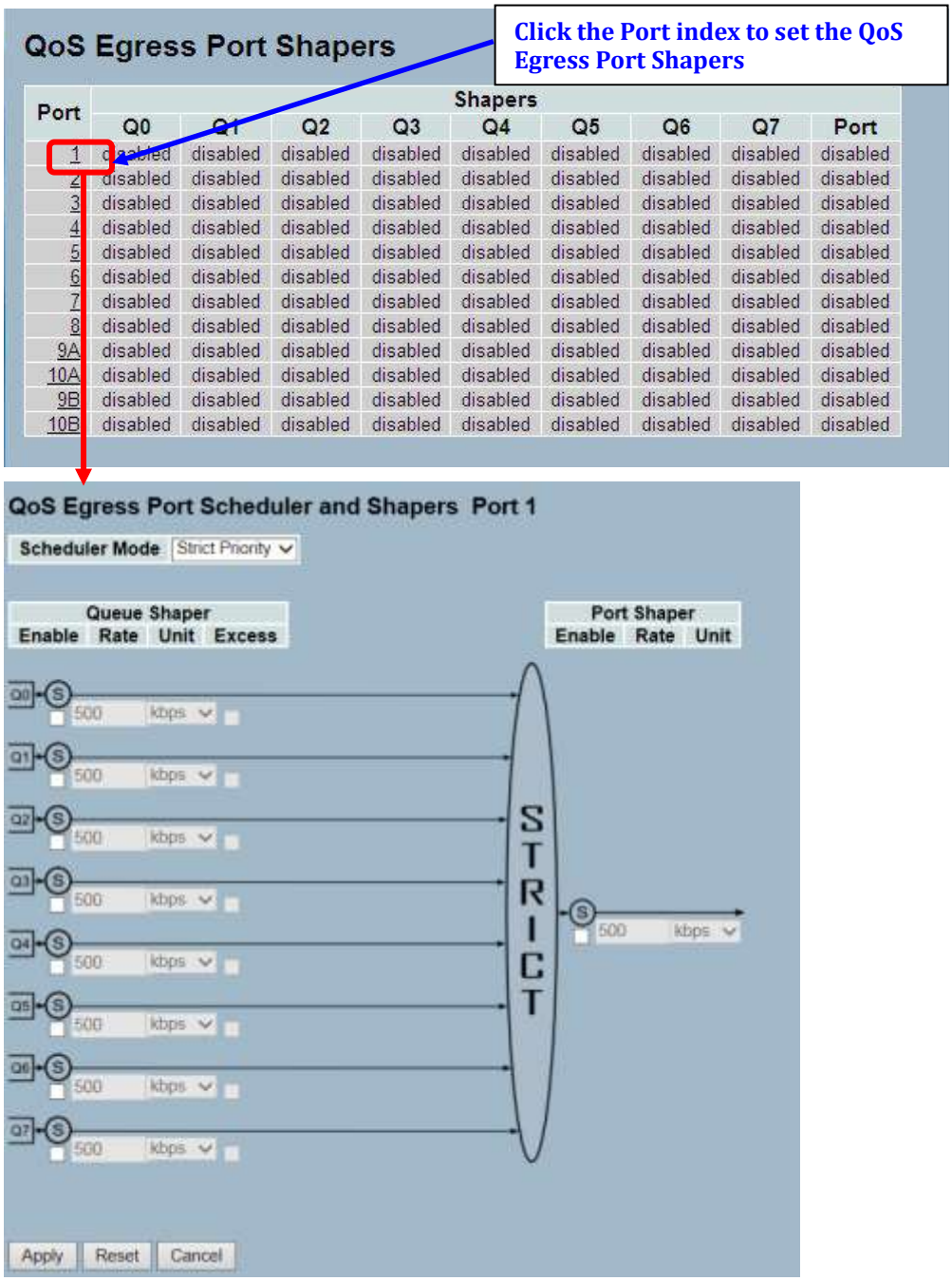
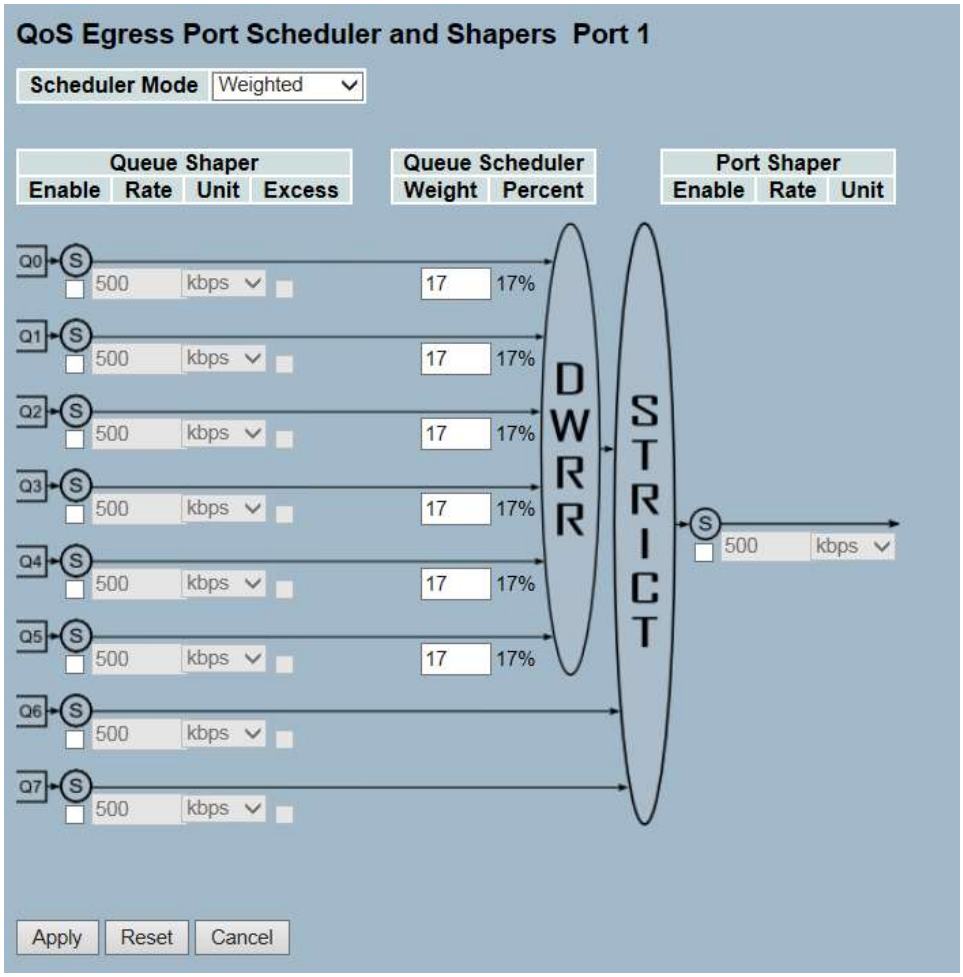

QoS Egress Port Shapers
Click the Port index to set the QoS Egress Port Shapers
Port
Shapers
Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Port
1 disabled disabled disabled disabled disabled disabled disabled disabled disabled
2 disabled disabled disabled disabled disabled disabled disabled disabled disabled
3 disabled disabled disabled disabled disabled disabled disabled disabled disabled
4 disabled disabled disabled disabled disabled disabled disabled disabled disabled
5 disabled disabled disabled disabled disabled disabled disabled disabled disabled
6 disabled disabled disabled disabled disabled disabled disabled disabled disabled
7 disabled disabled disabled disabled disabled disabled disabled disabled disabled
8 disabled disabled disabled disabled disabled disabled disabled disabled disabled
9A disabled disabled disabled disabled disabled disabled disabled disabled disabled
10A disabled disabled disabled disabled disabled disabled disabled disabled disabled
9B disabled disabled disabled disabled disabled disabled disabled disabled disabled
10B disabled disabled disabled disabled disabled disabled disabled disabled disabled
QoS Egress Port Scheduler and Shapers Port 1
Scheduler Mode
Strict Priority
Queue Shaper
Enable Rate Unit Excess
Port Shaper
Enable Rate Unit
Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7
500 kbps
STRICT
Apply
Reset
Cancel

Figure 3-15.4: The QoS Egress Port Shapers



Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Shapers (Qn): Shows "Disabled" or actual queue shaper rate (e.g. "800 Mbps").

Shapers (Port): Shows "Disabled" or actual port shaper rate (e.g. "800 Mbps").

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. The default value is “?”. This value is restricted to?-1000000, when the "Unit" is "Kbps". It is restricted to 1-?, when the "Unit" is "Mbps”.

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "Kbps" or "Mbps". The default value is "Kbps".

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only show if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. The default value is “?”. This value is restricted to ?-1000000, when the "Unit" is "Kbps". It is restricted to 1-?, when the "Unit" is "Mbps".

Port Shaper Unit: Controls the unit of measure for the port shaper rate as "Kbps" or "Mbps". The default value is "Kbps".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.5 Port Tag Remarking

The section provides an overview of QoS Egress Port Tag Remarking for all switch ports that belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Port Tag Remarking.

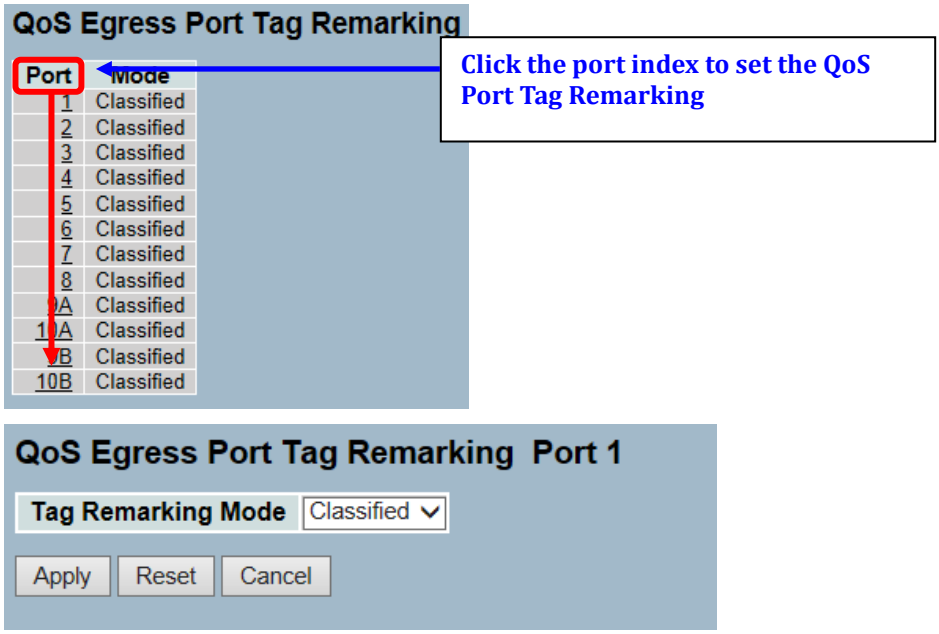


Figure 3-15.5: The Port Tag Remarking

Parameter Description

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

Mode: Shows the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.

Tag Remarking Mode: To scroll to select the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset-** Click "Reset" to undo any changes made locally and revert to previously saved values.
- **Cancel** – Click to cancel the changes.

3-15.6 Port DSCP

The section helps the user to set the basic QoS Port DSCP Configuration settings for all switch ports to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the web interface:

1. Click Configuration, QoS, Port DSCP.
2. Evoke to enable or disable the Ingress Translate and scroll the classify.
3. Parameter configuration.
4. Scroll to select Egress Rewrite parameters.
5. Click “Save” to save the setting.
6. If you want to cancel the setting, then you need to click the Reset button.
7. It will revert to previously saved values.

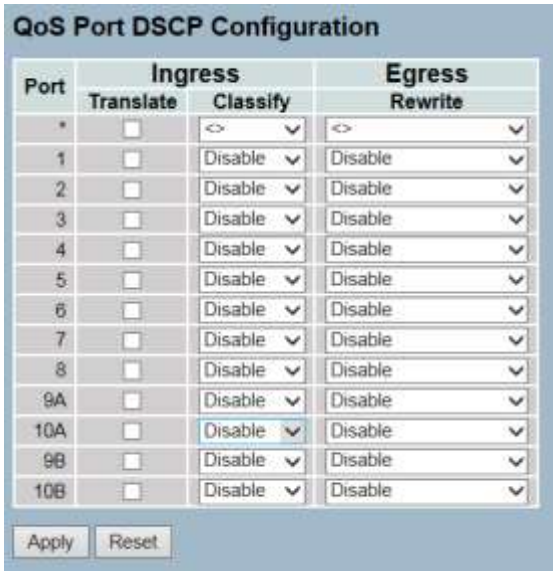


Figure 3-15.6: The QoS Port DSCP Configuration

Parameter Description

Port: The port column shows the list of ports that you can configure DSCP ingress and egress settings.

Ingress: In Ingress settings, you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. **Translate:** To enable the Ingress Translation, click the checkbox.
2. **Classify:** Classification for a port has 4 different values.

    - **Disable**: No Ingress DSCP Classification.
    - **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0.
    - **Selected**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
    - **All**: Classify all DSCP.

Egress: Port Egress Rewriting can be one of the following parameters:

- **Disable**: No Egress rewrite.
- **Enable**: Rewrite enable without remapped.
- **Remap**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.7 DSCP-Based QoS

The section helps the user configure the basic QoS, DSCP based, QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Evoke to enable or disable the DSCP for Trust.
3. Scroll to select QoS Class and DPL parameters.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

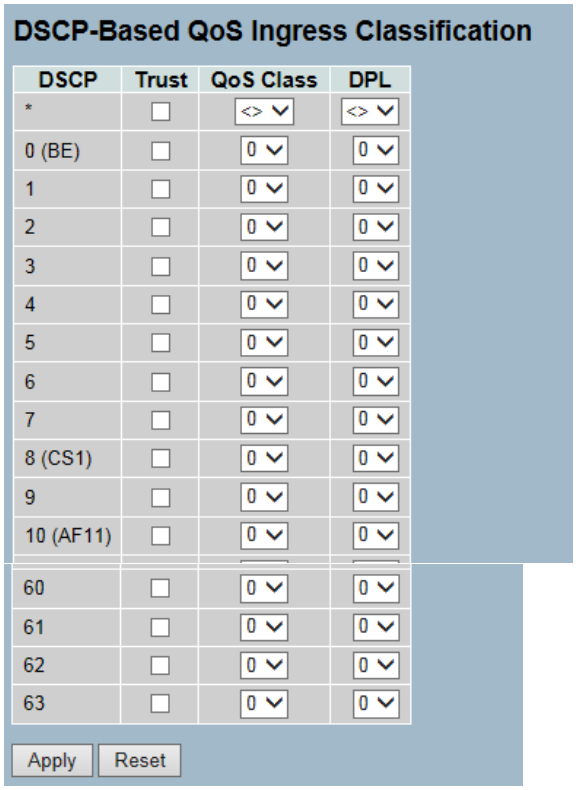


Figure 3-15.7: The DSCP-Based QoS Ingress Classification Configuration

Parameter Description

DSCP: Maximum number of supported DSCP values are 64.

Trust: Click to check if the DSCP value is trusted.

QoS Class: QoS Class value can be any of (0-7) .

DPL: Drop Precedence Level (0-3).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.8 DSCP Translation

The section allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Evoke to enable or disable classify.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

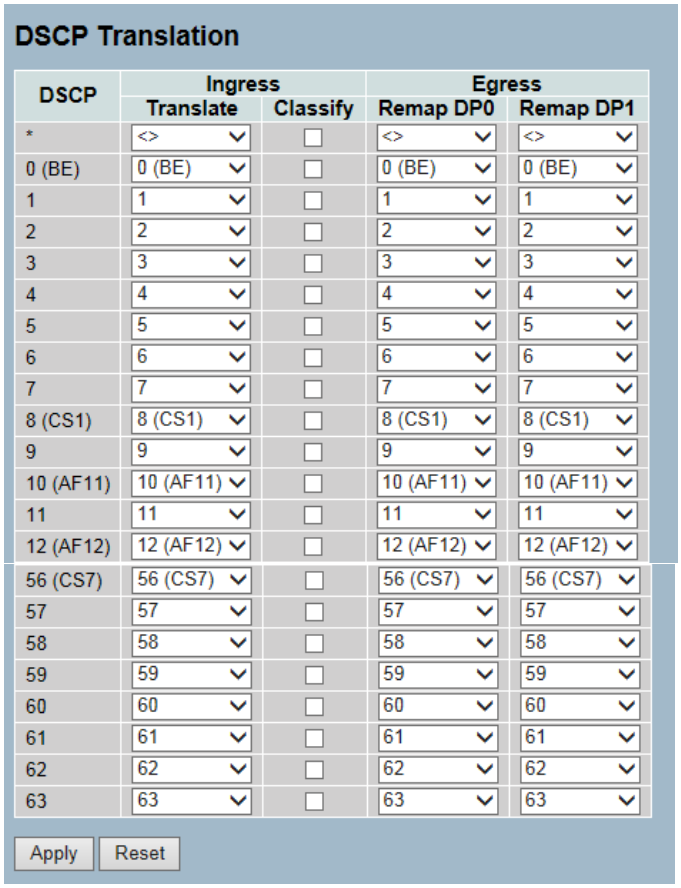


Figure 3-15.8: The DSCP Translation Configuration

Parameter Description

DSCP: The maximum number of supported DSCP values is 64 and the valid DSCP value ranges from 0 to 63.

Ingress: Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation –

1. **Translate:** DSCP at Ingress side can be translated to any of (0-63) DSCP values.
2. **Classify:** Click to enable classification at Ingress side.

Egress: There are following configurable parameters for Egress side –

1. **Remap DP0:** Selects the DSCP value from select menu that you want to remap. DSCP value ranges from 0 to 63.
2. **Remap DP1:** Select the DSCP value from select menu that you want to remap. DSCP value ranges from 0 to 63.

There is following configurable parameter for Egress side -

- **Remap:** Select the DSCP value from select menu that you want to remap. DSCP value ranges from 0 to 63.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.9 DSCP Classification

The section describes how to configure and map the DSCP value to a QoS class and DPL value. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. 1.Click Configuration, QoS, DSCP Classification.
2. Scroll to set the DSCP Parameters.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

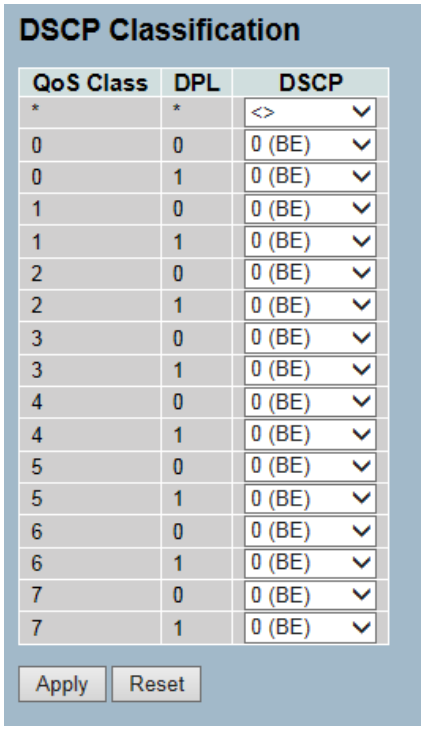


Figure 3-15.9: The DSCP Classification Configuration

Parameter Description

QoS Class: Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.

DPL: Drop Precedence Level (0-1) can be configured for all available QoS Classes.

DSCP: Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.10 QoS Control List Configuration

The section shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS, QoS Contol List.
2. Click the ⊕ to add a new QoS Control List.
3. Scroll all parameters and evoke the Port Member to join the QCE rules.
4. Click "Save" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

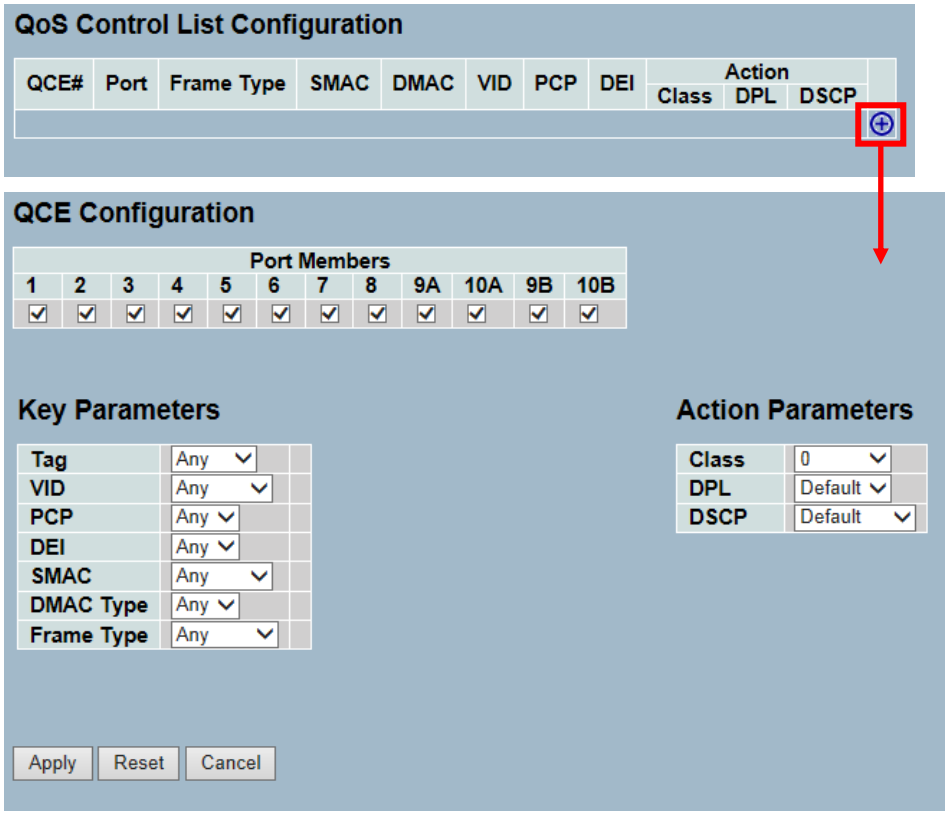


Figure 3-15.10: The QoS Control List Configuration

Parameter Description

QCE#: Indicates the index of QCE.

Port: Indicates the list of ports configured with the QCE.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

- **Any:** The QCE will match all frame type.
- **Ethernet:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
- **LLC:** Only (LLC) frames are allowed.
- **SNAP:** Only (SNAP) frames are allowed.
- **IPv4:** The QCE will match only IPV4 frames.
- **IPv6:** The QCE will match only IPV6 frames.

SMAC: Displays the OUI field of Source MAC address (e.g. first three octet (byte) of MAC address).

DMAC: Specifies the type of Destination MAC addresses for incoming frame. Possible values are:

- **Any:** All types of Destination MAC addresses are allowed.
- **Unicast:** Only Unicast MAC addresses are allowed.
- **Multicast:** Only Multicast MAC addresses are allowed.
- **Broadcast:** Only Broadcast MAC addresses are allowed.
- The default value is 'Any'.

VID: Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'.

PCP: Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI: Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1, or 'Any'.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

There are three action fields: Class, DPL, and DSCP.

- **Class:** Classified QoS Class; if a frame matches the QCE, it will be put in the queue.
- **DPL:** Drop Precedence Level; if a frame matches the QCE, then DP level will be set to the value displayed under the DPL column.
- **DSCP:** If a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.

Modification Buttons: You can modify each QCE (QoS Control Entry) in the table using the following buttons:

: Inserts a new QCE before the current row.

: Edits the QCE.

: Moves the QCE up the list.

: Moves the QCE down the list.

: Deletes the QCE.

: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members: Check the checkbox button to make any port member of the QCL entry. By default, all ports will be checked.

Key Parameters: Key configurations are described as below:

Tag Value of Tag field can be 'Any', 'Untag', or 'Tag'.

VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

SMAC Source MAC address: 24 MS bits (OUI) or 'Any'.

DMAC Type Destination MAC type: Possible values are unicast (UC), multicast (MC), broadcast (BC), or 'Any'.

Frame Type can have any of the following values:

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6

NOTE: All frame types are explained below:

1. **Any:** Allow all types of frames.
2. **Ethernet:** Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any'. The default value is 'Any'.
3. **LLC:** SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. The default value is 'Any'.
   DSAP Address Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. The default value is 'Any'.
   Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any'. The default value is 'Any'.
4. **SNAP:** PID Valid PID (a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any'. The default value is 'Any'.
5. **IPv4:** Protocol IP protocol number: (0-255, TCP, or UDP) or 'Any' Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255. When mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value, or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF, or AF11-AF43.

IP Fragment IPv4 frame fragmented option: yes|no|any
Sport Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

6. **IPv6:** Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'. Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits.

DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
Sport Source TCP/UDP port :(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Configuration:

Class QoS Class: "class (0-7)", default - basic classification.
DP Valid DP Level can be (0-3)", default - basic classification
DSCP Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43).

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-15.11 QCL Status

The section configures and shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Configuration, QoS , QCL Status.
2. If you want to auto-refresh the information, then you need to evoke the "Auto-Refresh".
3. Scroll to select the combined, static, Voice VLAN, and conflict.
4. To Click the "Refresh" to refresh an entry of the MVR Statistics Information.

Figure 3-15.11: The QoS Control List Status

Parameter Description

User: Indicates the QCL user.

QCE#: Indicates the index of QCE.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

- **Any**: The QCE will match all frame type.
- **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
- **LLC**: Only (LLC) frames are allowed
- **SNAP**: Only (SNAP) frames are allowed.
- **IPv4**: The QCE will match only IPV4 frames.
- **IPv6**: The QCE will match only IPV6 frames.

Port: Indicates the list of ports configured with the QCE.

Action: Indicates the classification action taken on ingress frame, if parameters configured are matched with the frame's content.

There are three action fields: Class, DPL, and DSCP.

- **Class**: Classified QoS Class; if a frame matches the QCE, it will be put in the queue.
- **DPL**: Drop Precedence Level; if a frame matches the QCE, then the DP level will be set to the value displayed under DPL column.
- **DSCP**: If a frame matches the QCE, then the DSCP will be classified with the value displayed under DSCP column.

Conflict: Displays QCE status. Resources required to add a QCE may not be available. In that case, it shows the conflict status as 'Yes'. Otherwise, it is always be 'No'. Please note that that conflict can be resolved by releasing the resource required by the QCE and pressing 'Refresh' button.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Resolve Conflict: Click it to resolve the conflict issue.

Upper right icon (Refresh): Click “Refresh” to refresh the QCL information manually.

3-15.12 Storm Control

The section configures the storm control for the switch. The types of controls are the unicast storm rate control, the multicast storm rate control, and the broadcast storm rate control. These only affect flooded frames (e.g. frames with a [VLAN ID, DMAC] pair not present on the MAC Address table). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS, Storm Control Configuration.
2. Evoke to select the frame type to enable storm control.
3. Scroll to set the Rate Parameters.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

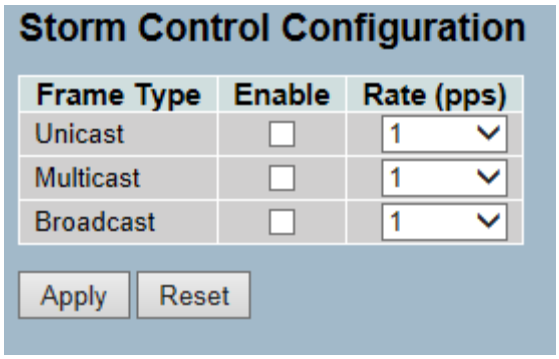


Figure 3-15.12: The Storm Control Configuration

Parameter Description

Frame Type: The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.

Enable: Enables or disables the storm control status for the given frame type.

Rate: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K, 1024K, 2048K, 4096K, 8192K, 16384K or 32768K, 1024K, 2048K, 4096K, 8192K, 16384K, or 32768K.

The 1 kpps is actually 1002.1 pps.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-16 S-Flow Agent

The sFlow Collector configuration for the switch can be monitored and modified. Up to 1 Collector is supported. This page allows configurations for the sFlow collector IP type, sFlow collector IP Address, Port Number, and for each sFlow Collector.

3-16.1 Collector

The "Current" field displays the currently configured sFlow Collector. The "Configured" field displays the new Collector Configuration.

Web Interface

To configure the sFlow Agent in the web interface:

1. Click Configuration, sFlow Agent, Collector.
2. Set the parameters.
3. Scroll to IP Type to choice with IPv4 or IPv6.
4. Click "Save" to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

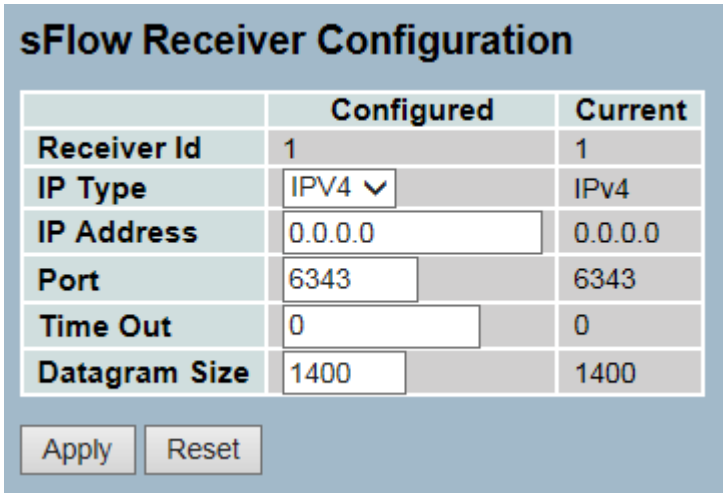


Figure 3-16.1: The sFlow Collector Configuration

Parameter Description

Receiver Id: The "Receiver ID" input fields allow the user to select the Collector ID. Indicates the ID of this particular sFlow Collector. Currently, one ID is supported as one collector is supported.

IP Type: A drop down list to select the type of IP of Collector is displayed. By default, IPv4 is the type of Collector IP type. You could use IPv4 or IPv6.

IP Address: The address of a reachable IP is to be entered into the text box. This IP is used to monitor the sFlow samples sent by sFlow Agent (our switch). By default, the IP is set to 0.0.0.0 and a new entry has to be added to it.

Port: A port that listens to the sFlow Agent has to be configured for the collector. The value of the port number has to be typed into the text box.

The value accepted is within the range of 1-65535. But an appropriate port number not used by other protocols need to be configured. By default, the port's number is 6343.

Time out: It is the duration during in which the collector receives samples. Once it is expired, the sampler stops sending samples. The value is set through the management before it expires. The value accepted is within the range of 0-2147483647. By default, it is set to 0.

Datagram Size: It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. The default is 1400 bytes.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-16.2 Sampler

You can set or edit the sFlow sampler to meet your requirements based on a defined sampling rate. An average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy.

Web Interface

To configure the sFlow Agent in the web interface:

1. Click Configuration, sFlow Agent, Sampler.
2. Click the to edit the sFlow sampler parameters.
3. Scroll to Sample Type to choice with None, Tx, Rx or All.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

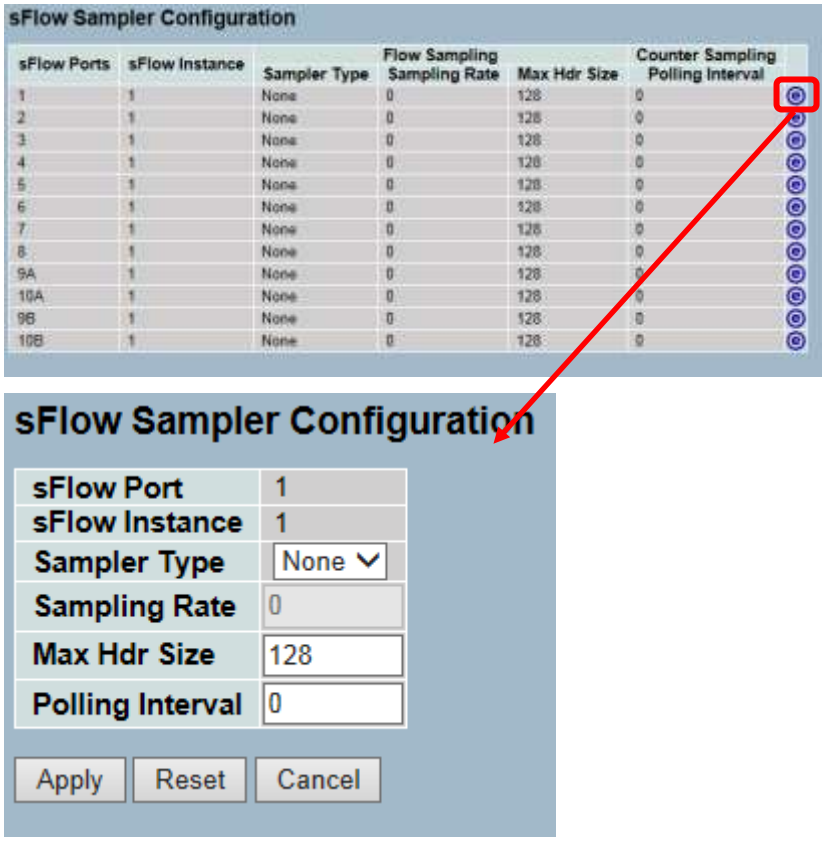


Figure 3-16.1: The sFlow sampler Configuration

Parameter Description

sFlow Ports: Lists of the port numbers on which sFlow is configured.

sFlow Instance: Configures sFlow instance for the port number.

Sampler Type: Configures sampler type on the port and could be any of the types: None, Rx, Tx, or All. You can scroll to choose one for your sampler type.

By default, the value is “None”.

Sampling Rate: Configures the sampling rate on the ports.

Max Hdr Size: Configures the size of the header of the sampled frame.

Polling Interval: Configures the polling interval for the counter sampling.

Buttons:

- - Edits the data source sampler configuration.
- **Apply** - Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the sFlow Sampler information manually.

3-17 Loop Protection

The Loop Protection is used to detect the presence of traffic. When switch receives the packet's (looping detection frame) MAC address (the same as oneself from the port), the loop protection happens. The port will be locked when it received the looping protection frames.

3-17.1 Configuration

The section describes how to set the loop protection.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection, Configuration.
2. Evoke to select enable or disable the port loop protection.
3. Click the apply to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

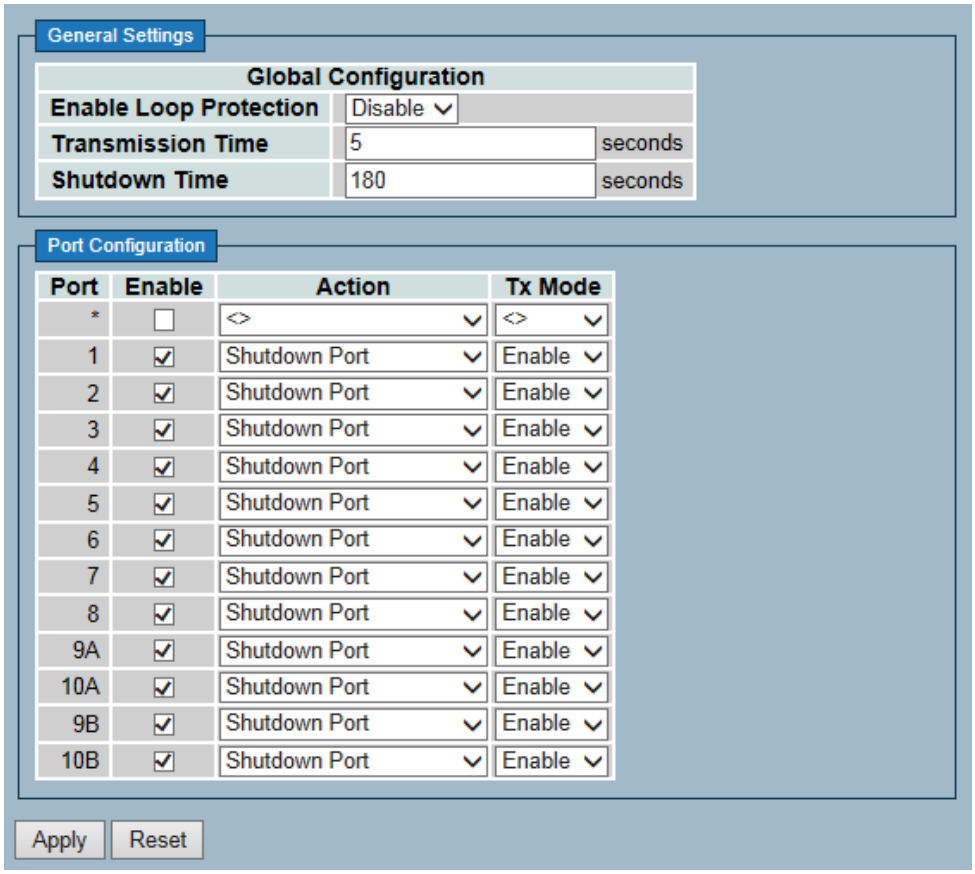


Figure 3-17.1: The Loop Protection Configuration.

Parameter Description

General Settings:

Enable Loop Protection: Controls whether loop protections is enabled (as a whole).

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration:

Port: The switch port number of the port.

Enable: Controls whether loop protection is enabled on this switch port.

Action: Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port, and Log or Log Only.

TX Mode: Controls whether the port is actively generating loop protection PDU's or whether it is just passively looking for looped PDU's.

Buttons:

- **Apply** – Click to apply changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

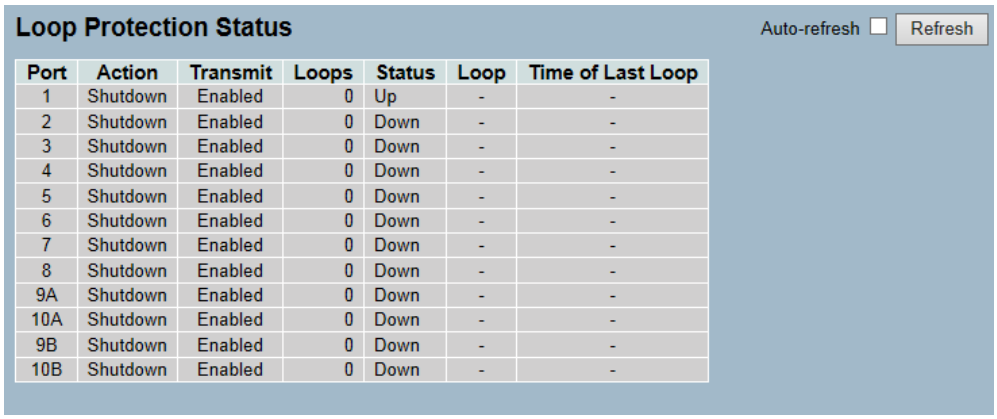
3-17.2 Status

This page displays the loop protection port status of the switch.

Web Interface

To configure the loop protection status parameters in the web interface:

1. Click Configuration, Loop Protection, Status.
2. Evoke the auto-refresh or click to refresh the loop protection port status manually.



Loop Protection Status

Auto-refresh ☐ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9A	Shutdown	Enabled	0	Down	-	-
10A	Shutdown	Enabled	0	Down	-	-
9B	Shutdown	Enabled	0	Down	-	-
10B	Shutdown	Enabled	0	Down	-	-

Figure 3-17.2: The Loop Protection Status.

Parameter Description

Port: The switch port number of the logical port.

Action: The currently configured port action.

Transmit: The currently configured port transmit mode.

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port.

Loop: Whether a loop is currently detected on the port.

Time of Last Loop: The time of the last loop event detected.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the Loop Protection information manually.

3-18 Single IP

Provides a single IP address management of up to 32 switches. It is not limited to specific models, distance barriers, specialized cables, or stacking method.

3-18.1 Configuration

Each single IP group consists of one master switch and up to 32 slave switches. The master switch is used as an agent to manage all the switches in the same group. The slave switch is a switch that want to join a single IP group. It could be accessed from the master switch.

Web Interface

To configure the single IP parameters in the web interface:

1. Click Configuration, Single IP, Configuration.

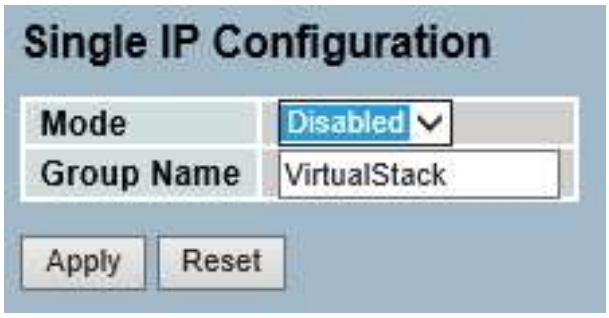


Figure 3-19.1: The Single IP Configuration.

Parameter Description

Mode: Possible modes are:

- **Disable**: Disables operation of Single IP Management.
- **Master**: Enables Single IP Management and to be a Master Switch.
- **Slave**: Enables Single IP Management and to be a Slave Switch.

Group Name: Indicates the name of the Single IP group. Maximum length of the Group Name String is 64.

Buttons:

- **Apply** – Click to apply changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-18.2 Information

Displays the active Slave Switch information.

Web Interface

To configure the Single IP parameters in the web interface:

1. Click Configuration, Single IP, Information.
2. Evoke the auto-refresh or click to refresh the Single IP slave member manually.

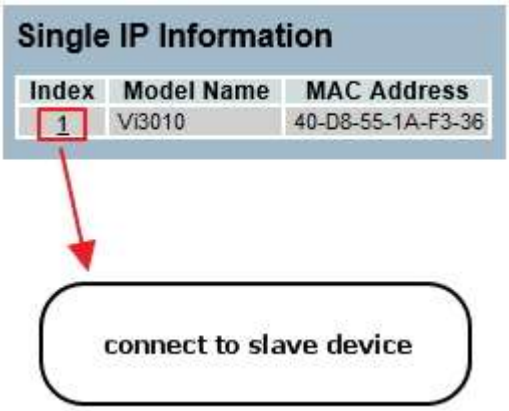


Figure 3-19.2: The Single IP Information.

Parameter Description

Index: The ID of the active Slave Switch.

Model Name: Displays the model name of the Slave Switch.

MAC Address: Displays the Ethernet MAC address of the Slave Switch.

Buttons:

- **Refresh-** Updates the Single IP information.

3-19 Easy Port

Easy Port provides a convenient way to save and share common configurations. You can use it to enable features and settings, based on the location of a switch in the network and for mass configuration deployments across the network. You could easily implement Voice IP Phones, Wireless Access Points, IP Cameras, and more. You can also leverage configuration to run a converged voice, video, and data network, considering quality of service (QoS), bandwidth, latency, and high performance.

Web Interface

To configure the Easy Port in the web interface:

1. Click Configuration, Easy Port.
2. Set the parameters.
3. Scroll to select what kind device you want to set on the Easy Port and connect to.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

NOTE: The easy port configuration page will not actively display the status of setting. The page is for configuring each parameter, so it is correct if the parameter isn’t modified after the selection of each item is applied. The modification will show on the configuration of individual functionality.

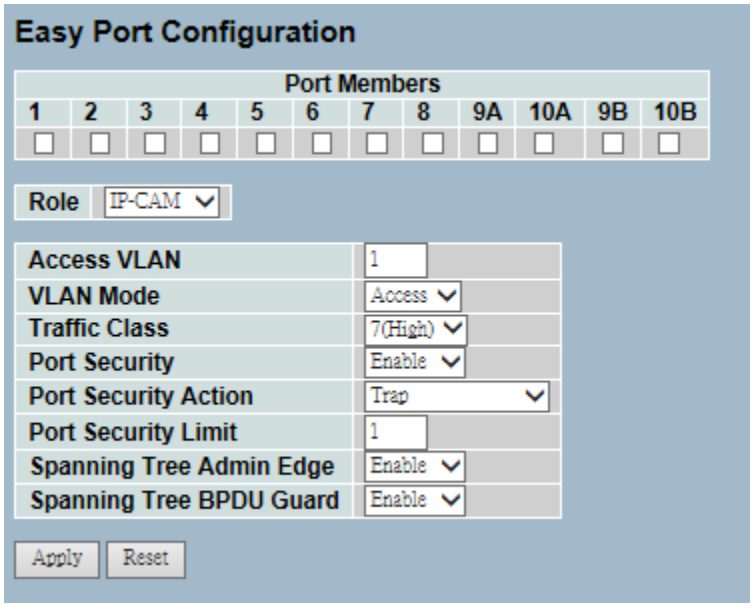


Figure 3-19.1: The Easy Port Configuration

Parameter Description

Port Members: To evoke which port wants to enable the Easy Port function.

Role: Scroll to select what kind device you want to connect and implement with the Easy Port setting.

Access VLAN: To set the Access VLAN ID means that the switch port access VLAN ID (AVID).

VLAN Mode: Scroll to select the VLAN mode with Access, Trunk, or Hybrid.

Traffic Class: Scroll to select the traffic class for the data stream priority. The available value is from 0 (Low) to 7 (High). If you want the voice has high priority, then you can set the value with 7.

Port Security: Scroll to enable or disable the port security function on the port. If you turn on the function, then you need to set port security limit to allow how many device can access the port (via MAC address).

Port Security Action: Scroll to select when the device wasn't allow to access, then switch action as trap, shutdown, or trap & shutdown.

Port Security limit: To set the port security limit (it means you can set how many device MAC address will allow to access the port). The default is 1.

Spanning Tree Admin Edge: Scroll to enable or disable the Spanning Tree Admin Edge function on the Easy Port.

Spanning Tree BPDU Guard: Scroll to enable or disable the Spanning Tree BPDU Guard function on the Easy Port.

Buttons:

- **Apply** – Click "Apply" to save changes.
- **Reset-** Click "Reset" to undo any changes made locally and revert to previously saved values.

3-20 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively. Thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, Mirroring.
2. Scroll to select which port to mirror.
3. Scroll to disabled, enable, TX Only, and RX Only to set the Port mirror mode.
4. Click “Save” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

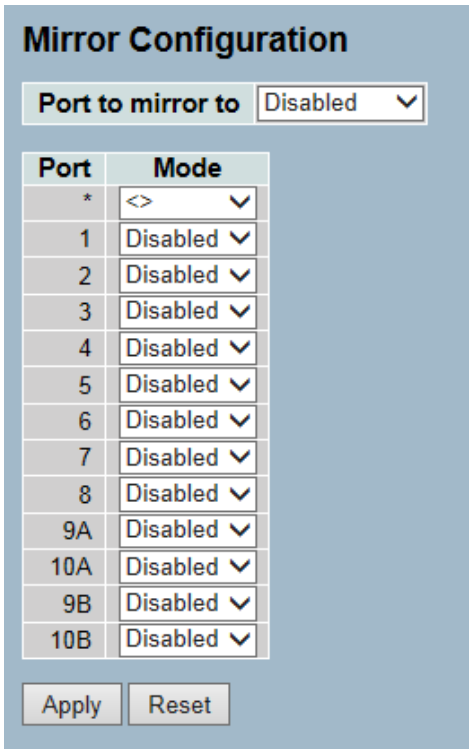


Figure 3-20.1: The Mirror Configuration

Parameter Description

Port to mirror on: Port to mirror, also known as, the mirror port. Frames from ports that have either source (Rx) or destination (Tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port: The logical port for the settings contained in the same row.

Mode: Select mirror mode.

Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled Neither frames transmitted nor frames received are mirrored.

Enabled Frames received and frames transmitted are mirrored on the mirror port.

NOTE: For a given port, a frame is only transmitted once. Therefore, it is not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to Disabled or Rx only.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-21 Trap Event Severity

The Trap Event Severity function is used to set an alarm trap and get the event log. The Trap Events Configuration function is used to enable the switch to send out the trap information, while pre-defined trap events occurred.

Web Interface

To configure the Trap Event Severity Configuration in the web interface:

1. Click Configuration, Trap Event Severity Configuration.
2. Scroll to select the Group name and Severity Level.
3. Click “Save” to save the setting.
4. If you want to cancel the setting, click the reset button to revert back to previously saved values.

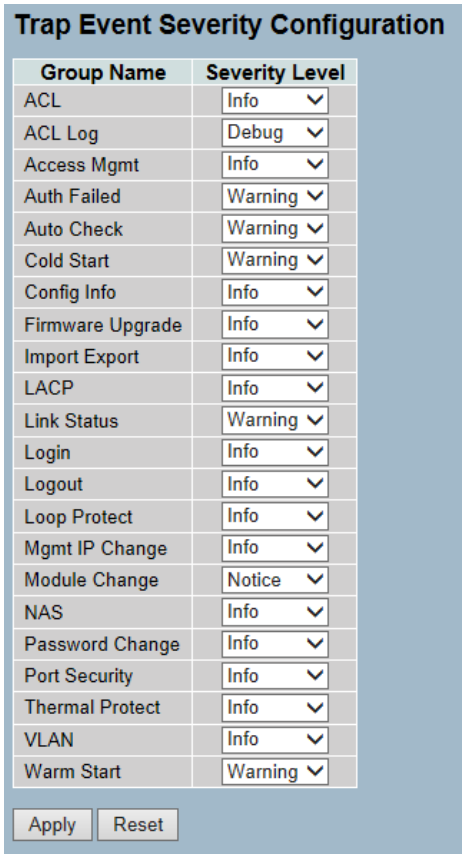


Figure 3-21.1: The Trap Event Severity Configuration

Parameter Description

Group Name: The field describes the Trap Event definition.

Severity Level: Every group has a severity level. The following level types are supported:

<0> Emergency: System is unusable.

<1> Alert: Action must be taken immediately.

<2> Critical: Critical conditions

<3> Error: Error conditions

<4> Warning: Warning conditions

<5> Notice: Normal but significant conditions

<6> Information: Information messages

<7> Debug: Debug-level messages

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

3-22 UpnP

UPnP is an acronym for Universal Plug-and-Play. The goals of UPnP are to allow devices to connect seamlessly, and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration, UpnP.
2. Scroll to select the mode to enable or disable.
3. Specify the parameters in each blank field.
4. Click “Apply” to save the setting.
5. If you want to cancel the setting, click the reset button to revert back to previously saved values.

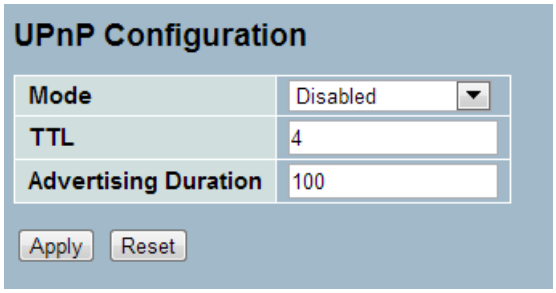


Figure 3-23.1: The UPnP Configuration

Parameter Description

These parameters are displayed on the UPnP Configuration page:

Mode: Indicates the UPnP operation mode. Possible modes are:

- **Enabled:** Enables UPnP mode operation.
- **Disabled:** Disables UPnP mode operation.
- When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points on how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it assumes that the switch no longer exists. Due to the unreliable nature of UDP, it is standardly recommended that a refreshment of advertisements should be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons:

- **Apply** – Click to apply changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

Chapter 4: Security

This chapter describes all of the switch security configuration tasks to enhance the security of local network including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, and so on.

4-1 Source Guard

The section describes the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configuration to enable or disable with the port of the switch.

4-1.1 Configuration

This section describes how to configure IP Source Guard setting including:

- Mode (Enabled and Disabled)
- Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Select “Enabled” in the mode of IP Source Guard Configuration.
2. Select “Enabled” of the specific port in the mode of Port Mode Configuration.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
4. Click “Apply”.

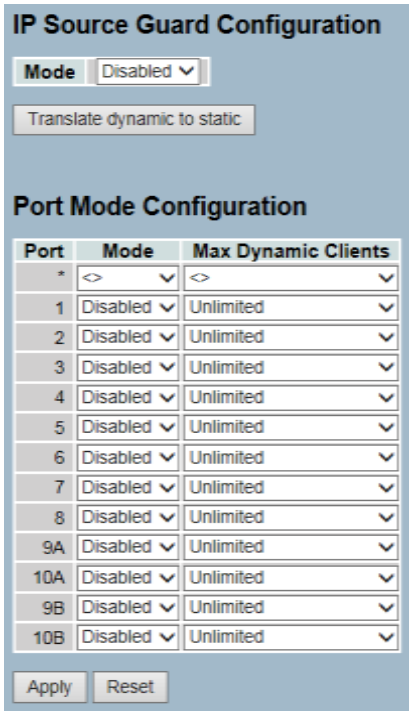


Figure 4-1.1: The IP Source Guard Configuration

Parameter Description

Mode of IP Source Guard Configuration: Enables or disables the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration: Specifies which port the IP Source Guard is enabled on. Only when both Global Mode and Port Mode on a given port are enabled, then the IP Source Guard is enabled on this given port.

Max Dynamic Clients: Specifies the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2, or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, then it only allows the IP packets forwarding that matched in static entries on the specific port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-1.2 Static Table

The section describes the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configuration to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click “Add New Entry”.
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click “Apply”.

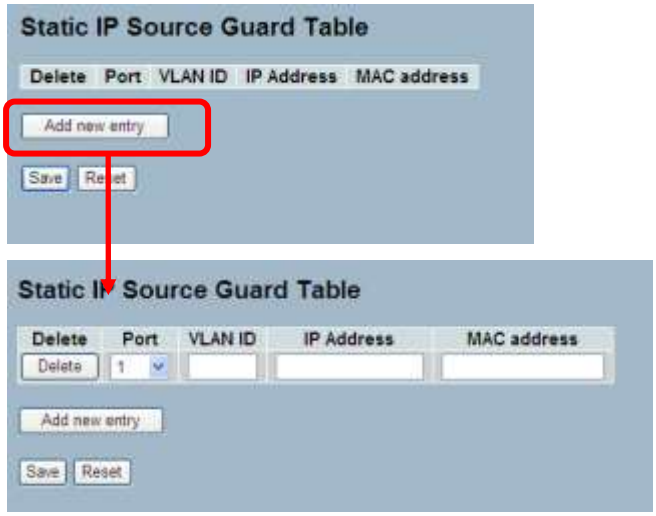


Figure 4-1.2: The Static IP Source Guard Table

Parameter Description

Delete: Check to delete the entry. It will be deleted during the next save.

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

IP Address: Allowed Source IP address.

MAC address: Allowed Source MAC address.

Adding new entry: Click to add a new entry to the Static IP Source Guard table. Specifies the port, VLAN ID, IP address, and IP mask for the new entry. Click "Save".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-1.3 Dynamic Table

The section describes the Dynamic IP Source Guard Table parameters of the switch. You could use the Dynamic IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the web interface:

1. Specify the “Start” from port, VLAN ID, IP Address, and entries per page.
2. Checked “Auto-Refresh”.

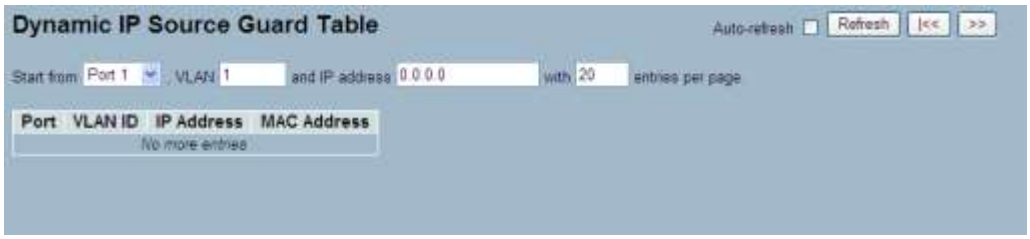


Figure 4-1.3: The Dynamic Table

Parameter Description

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN ID in which the IP traffic is permitted.

IP Address: User IP address of the entry.

MAC Address: Source MAC address.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the Dynamic IP Source Guard Table manually. Click **“<<”** or **“>>”** to move to the next or previous page.

4-2 ARP Inspection

The section describes the ARP Inspection parameters of the switch. You could use the ARP Inspection configuration to manage the ARP table.

4-2.1 Configuration

This section describes how to configure the ARP Inspection setting including:

- Mode (Enabled and Disabled)
- Port (Enabled and Disabled)

Web Interface

To configure the ARP Inspection Configuration in the web interface:

1. Select “Enabled” in the Mode of ARP Inspection Configuration.
2. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
3. Click “Apply”.

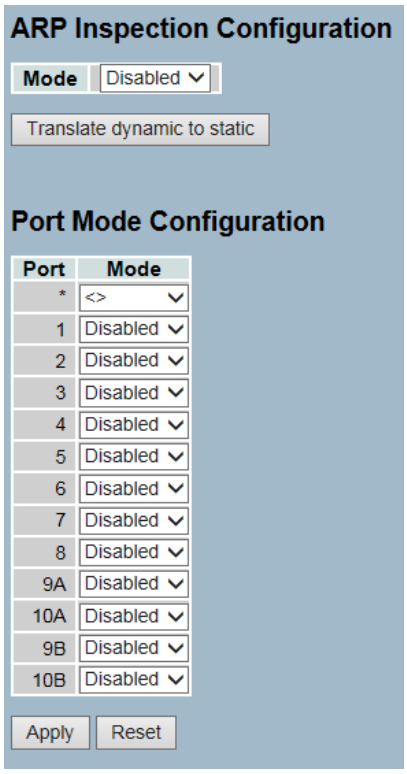


Figure 4-2.1: The ARP Inspection Configuration

Parameter Description

Mode of ARP Inspection Configuration: Enables or disables the Global ARP Inspection.

Port Mode Configuration: Specifies which ports the ARP Inspection is enabled on. Only when both Global Mode and Port Mode on a given port are enabled, then the ARP Inspection is enabled on this given port.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset**- Click “Reset” to undo any changes made locally and revert to previously saved values.

4-2.2 Static Table

The section describes the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table configuration to manage the ARP entries.

Web Interface

To configure the Static ARP Inspection Table Configuration in the web interface:

1. Click “Add New Entry”.
2. Specify the port, VLAN ID, IP address, and MAC address in the entry.
3. Click “Apply”.

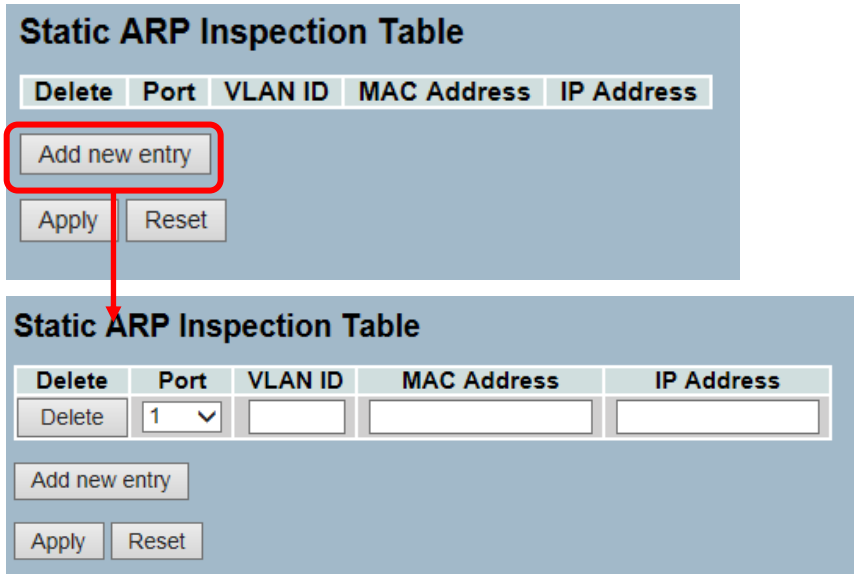


Figure 4-2.2: The Static ARP Inspection Table

Parameter Description

Delete: Check to delete the entry. The entry will be deleted during the next save.

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

MAC Address: The allowed Source MAC address in ARP request packets.

IP Address: The allowed Source IP address in ARP request packets.

Adding new entry: Click to add a new entry to the Static ARP Inspection table. Specify the port, VLAN ID, MAC address, and IP address for the new entry. Click "Apply".

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-2.3 Dynamic Table

The section describes the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries. The table is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Specify the “Start” from port, VLAN ID, MAC Address, IP Address, and entries per page.
2. Checked “Auto-Refresh”.

Figure 4-2.3: The Dynamic ARP Inspection Table

Parameter Description

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh, <<, >>): Click “Refresh” to refresh the Dynamic ARP Inspection Table manually. Click **“<<”** or **“>>”** to move to the next or previous page.

4-3 DHCP Snooping

The section describes the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

4-3.1 Configuration

This section describes how to configure the DHCP Snooping setting including:

- Snooping Mode (Enabled and Disabled)
- Port Mode Configuration (Trusted and Untrusted)

Web Interface

To configure a DHCP Snooping in the web interface:

1. Select “Enabled” in the Mode of DHCP Snooping Configuration.
2. Select “Trusted” of the specific port in the Mode of Port Mode Configuration.
3. Click “Apply”.

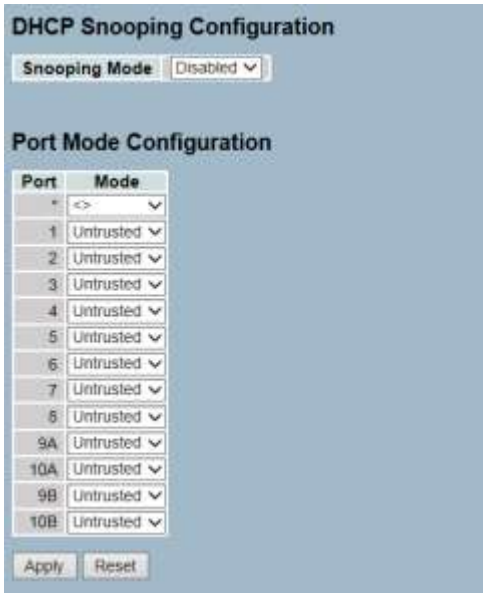


Figure 4-3.1: The DHCP Snooping Configuration

Parameter Description

Snooping Mode: Indicates the DHCP snooping mode operation. Possible modes are:

- **Enabled:** Enables the DHCP snooping mode operation. When the DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
- **Disabled:** Disables the DHCP snooping mode operation.

Port Mode: Indicates the DHCP snooping port mode. Possible port modes are:

- **Trusted:** Configures the port as trusted source of the DHCP messages.
- **Untrusted:** Configures the port as untrusted source of the DHCP messages.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-3.2 Statistics

The section describes to show the DHCP Snooping Statistics information of the switch. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. It doesn't count the DHCP packets for DHCP client.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the web interface:

1. Specify the port that you want to monitor.
2. Checked “Auto-Refresh”.

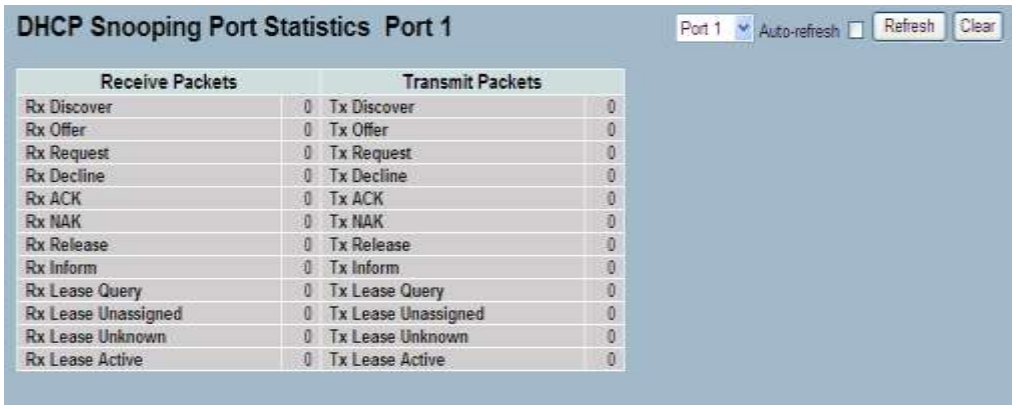


Figure 4-3.2: The DHCP Snooping Port Statistics

Parameter Description

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh, Clear): Click “Refresh” to refresh the DHCP Snooping Port Statistics manually. Click “Clear” to clean up the entries.

4-4 DHCP Relay

The section describes how to forward the DHCP requests to another specific DHCP server via DHCP relay. The DHCP servers may be on another network.

4-4.1 Configuration

This section describes how to configure DHCP Relay setting including:

- Relay Mode (Enabled and Disabled)
- Relay Server IP Setting
- Relay Information Mode (Enabled and Disabled)
- Relay Information Mode Policy (Replace, Keep, and Drop)

Web Interface

To configure a DHCP Relay in the web interface:

1. Select “Enabled” in the Relay Mode of DHCP Relay Configuration.
2. Specify the Relay Server IP address.
4. Select “Enabled” in the Relay Information Mode of DHCP Relay Configuration.
5. Specify Relay (Replace, Keep, and Drop) in the Relay Information Mode of DHCP Relay Configuration.
6. Click “Apply”.

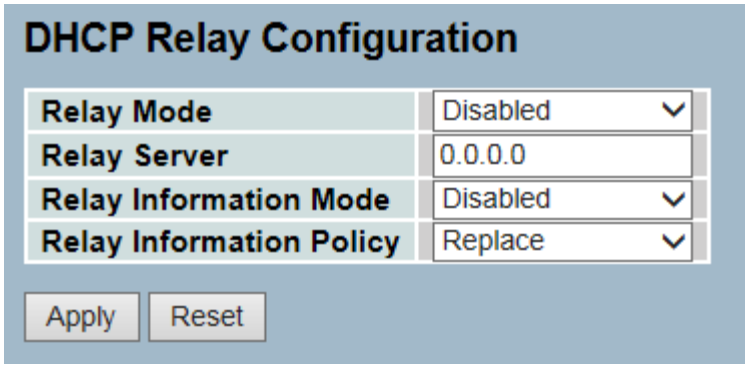


Figure 4-4.1: The DHCP Relay Statistics

Parameter Description

Relay Mode: Indicates the DHCP relay mode operation. Possible modes are:

- **Enabled:** Enables the DHCP relay mode operation. When the DHCP relay mode operation is enabled, the agent forwards and transfers the DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
- **Disabled:** Disables the DHCP relay mode operation.

Relay Server: Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer the DHCP messages between the clients and the server when they are not in the same subnet domain.

Relay Information Mode: Indicates the DHCP relay information mode option operation. Possible modes are:

- **Enabled:** Enables the DHCP relay information mode operation. When t he DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to the DHCP server. The agent removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
- **Disabled:** Disables the DHCP relay information mode operation.

Relay Information Policy: Indicates the DHCP relay information option policy. When the DHCP relay information mode operation is enabled and if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. It only works under DHCP if the relay information operation mode is enabled. Possible policies are:

- **Replace:** Replaces the original relay information when a DHCP message that already contains it is received.
- **Keep:** Keeps the original relay information when a DHCP message that already contains it is received.
- **Drop:** Drops the package when a DHCP message that already contains relay information is received.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-4.2 Statistics

The section describes the DHCP Relay Statistics information of the switch. The statistics show both of the server and client packet counters when the DHCP Relay mode is enabled.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the web interface:

1. Checked “Auto-Refresh”.

Figure 4-4.2: The DHCP Relay Statistics

Parameter Description

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Server: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known Circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error, while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets which were replaced with the relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped, which were received with relay agent information.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh, Clear): Click “Refresh” to refresh the DHCP Relay Statistics manually. Click “Clear” to clean up the entries.

4-5 NAS

The section describes the NAS parameters of the switch. The NAS server can be employed to connect users to a variety of resources including internet access, conference calls, printing documents on shared printers, or by simply logging on to the internet.

4-5.1 Configuration

This section describes how to configure the NAS setting of IEEE 802.1X, MAC-based authentication system, and port settings. The NAS configuration consists of two sections: a system-wide and a port-wide.

Web Interface

To configure a System Configuration of Network Access Server in the web interface:

1. Select “Enabled” in the Mode of Network Access Server Configuration.
2. Checked “Reauthentication Enabled”.
3. Set Reauthentication Period (the default is 3600 seconds).
4. Set the EAPOL Timeout (the default is 30 seconds).
5. Set the Aging Period (the default is 300 seconds).
6. Set the Hold Time (the default is 10 seconds).
7. Checked RADIUS-Assigned QoS Enabled.
8. Checked RADIUS-Assigned VLAN Enabled.
9. Checked Guest VLAN Enabled.
10. Specify the Guest VLAN ID.
11. Specify the Max Reauth Count.
12. Checked “Allow Guest VLAN” if EAPOL is seen.
13. Click “Apply”.

Figure 4-5.1: The Network Access Server Configuration

Parameter Description

Mode: Indicates if the NAS is globally enabled or disabled on the switchstack. If it is globally disabled, all ports are allowed to forward the frames.

Reauthentication Enabled: If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the “Reauthentication Period”. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client. Therefore, it doesn't imply that a client is still present on a port (see “Aging Period” below).

Reauthentication Period: Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the “Reauthentication Enabled” checkbox is checked. The valid values are in the range 1 to 3600 seconds.

EASPOL Timeout: Determines the time for retransmission of “Request Identity EAPOL Frames”.

The valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

Aging Period: This setting applies to the following modes (e.g. modes using the port security functionality to secure MAC addresses):

- **Single 802.1X**
- **Multi 802.1X**
- **MAC-Based Auth**

When the NAS module uses the port security module to secure MAC addresses, the port security module needs to check for activity on the MAC address in question at regular intervals, and free any resources if there is no activity within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not critical since the supplicants are no longer attached to the port. They will get removed upon the next failed reauthentication. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client. This will not detect whether the client is still attached or not. The only way to free any resources is to age the entries.

Hold Time: This setting applies to the following modes (e.g. modes using the port security functionality to secure MAC addresses):

- **Single 802.1X**
- **Multi 802.1X**
- **MAC-Based Auth.**

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the “Unauthorized” state. The hold timer does not count during an on-going authentication.

In “MAC-based Auth.” mode, the switch will ignore any new frames coming from the client during the hold time.

The hold time can be set to a number between 10 and 1000000 seconds.

RAUDIUS-Assigned QoS Enabled: The RADIUS-assigned QoS provides a means to centrally control the traffic class, to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see “RADIUS-Assigned QoS Enabled” below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to, and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see “RADIUS-Assigned VLAN Enabled” below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled: A Guest VLAN is a special VLAN, typically with limited network access, which 802.1X-unaware clients are placed on after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the “Guest VLAN” as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable the Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID: This is the value that a port's Port VLAN ID is set to, if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

The valid values are in the range of 1 to 4095.

Max. Reauth. Count: The Max. Reauth. Count is the number of times the switch transmits an EAPOL request identity frame without response before entering the Guest VLAN. The value can only be changed if the Guest VLAN option is globally enabled.

The valid values are in the range of 1 to 255.

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN, even if an

EAPOL frame has been received on the port for the lifetime of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration: The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Port: The port number for which the configuration below applies.

Admin State: If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

- **Force Authorized:** In this mode, the switch will send one EAPOL success frame when the port link comes up and any client on the port will be allowed network access without authentication.
- **Force Unauthorized:** In this mode, the switch will send one EAPOL failure frame when the port link comes up and any client on the port will be disallowed network access.
- **Port-Based 802.1X:** In the 802.1X world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the middle man, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible. It allows different authentication methods such as MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When the authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open or block traffic on the switch port connected to the supplicant.

NOTE: Supposed two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page). Also supposed that the first server in the list is currently down (but not considered dead).

Now, if the supplicant retransmits EAPOL start frames at a rate faster than X seconds, then it will never get authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL start frame from the supplicant.

Since the server hasn't failed yet (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL start frame retransmission rate.

- **Single 802.1X:** Once a supplicant is successfully authenticated on a port in a port-based 802.1X authentication, the whole port is opened for network traffic. This allows other clients connected to the port (e.g. through a hub) to piggy-back on the successfully authenticated client and get network access even though they aren't really authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, only one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secured mode. In this mode, the port security module is used to secure a supplicant's MAC address once it’s successfully authenticated.
- **Multi 802.1X:** Once a supplicant is successfully authenticated on a port in a port-based 802.1X authentication, the whole port is opened for network traffic. This allows other clients connected to the port (e.g. through a hub) to piggy-back on the successfully authenticated client and get network access even though they aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is, like Single 802.1X, not an IEEE standard but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the port security module.

In the Multi 802.1X mode, it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant. This would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL start or EAPOL response identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL request identity frames by using the BPDU multicast MAC address as destination to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited by using the port security limit control functionality.

- **Mac-Based Auth:** Unlike the port-based 802.1X, the MAC-based authentication is not a standard. It is merely a best-practices method adopted by the industry. In a MAC-based authentication, users are called clients and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx". A dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When the authentication is complete, the RADIUS server sends a success or failure indication, which causes the switch to open or block traffic for that particular client using the port security module. Only then, will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication. Therefore, the MAC-based authentication has nothing to do with the 802.1X standard.

  The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. The maximum number of clients that can be attached to a port can be limited using the port security limit control functionality.

- **RADIUS-Assigned QoS Enabled:** When the RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port; the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If it’s present and valid, the traffic received on the supplicant's port will be classified to the given QoS Class. If (re-) authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator without affecting the RADIUS-assigned).

This option is only available for single-client modes:

- **Port-Based 802.1X**
- **Single 802.1X**

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered to be valid. It must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range 0 to 3, which translates into the desired QoS Class in the range of 0 to 3.

- **RADIUS-Assigned VLAN Enabled:** When the RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If it's present and valid, the port's Port VLAN ID will be changed to this VLAN ID. The port will be set to be a member of that VLAN ID and will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

  If (re-) authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator without affecting the RADIUS-assigned).

  This option is only available for single-client modes:

  - **Port-based 802.1X**
  - **Single 802.1X**

  To trouble-shoot VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  RADIUS attributes used in identifying a VLAN ID:

  RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

  - The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
  - The switch looks for the first set of these attributes that have the same tag value and fulfill the following requirements (if tag = 0 is used, the Tunnel-Private-Group-ID does not need to include a tag).
    - The value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
    - The value of Tunnel-Type must be set to "VLAN" (ordinal 13).

        - The value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range 0 to 9, which is interpreted as a decimal string to represent the VLAN ID. Leading '0's are discarded. The final value must be in the range of 1 to 4095.
- **Guest VLAN Enabled:** When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

  This option is only available for EAPOL-based modes:

  - **Port-based 802.1X**
  - **Single 802.1X**
  - **Multi 802.1X**

  To trouble-shoot VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  Guest VLAN Operation:

  When a Guest VLAN enabled port's link comes up, the switch starts to transmit EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and meanwhile no EAPOL frames have been received, the switch considers entering the Guest VLAN. The interval between the transmission of EAPOL request identity frames is configured with EAPOL timeout. If “Allow Guest VLAN if EAPOL Seen” is enabled, the port will now be placed in the Guest VLAN. If it’s disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed) and if not, the port will be placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN but continue transmitting EAPOL request identity frames at the rate given by the EAPOL timeout.

  Once in the Guest VLAN, the port is considered authenticated and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL success frame when entering the Guest VLAN.

  While in the Guest VLAN, the switch monitors the link for EAPOL frames. If such a frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

- **Port State:** The current state of the port. It can undertake one of the following values:
  - **Globally Disabled:** NAS is globally disabled.
  - **Link Down**: NAS is globally enabled, but there is no link on the port.
  - **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
  - **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
  - **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

- **Restart:** Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

  Clicking these buttons will not cause settings changed on the page to take effect.

  - **Reauthenticate**: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For a MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
  - **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

Upper right icon (Refresh): Click “Refresh” to refresh the NAS Configuration manually.

4-5.2 Switch Status

The section describes each port's NAS status information of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the web interface:

1. Checked "Auto-Refresh".

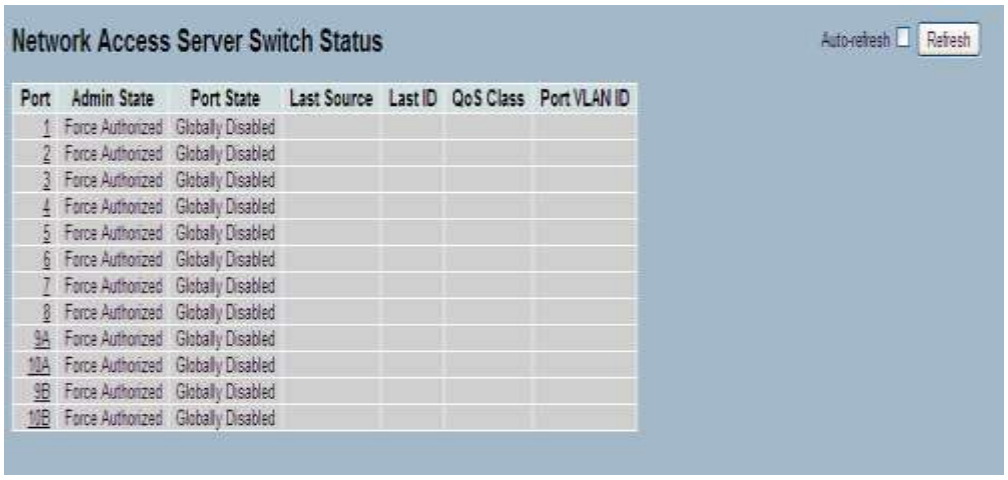

Network Access Server Switch Status
Auto-refresh
Refresh
Port Admin State Port State Last Source Last ID QoS Class Port VLAN ID
1 Force Authorized Globally Disabled
2 Force Authorized Globally Disabled
3 Force Authorized Globally Disabled
4 Force Authorized Globally Disabled
5 Force Authorized Globally Disabled
6 Force Authorized Globally Disabled
7 Force Authorized Globally Disabled
8 Force Authorized Globally Disabled
9A Force Authorized Globally Disabled
10A Force Authorized Globally Disabled
9B Force Authorized Globally Disabled
10B Force Authorized Globally Disabled

Figure 4-5.2: The Network Access Server Switch Status

Parameter Description

Port: The switch port number. Click for more detailed NAS statistics for this port.

Admin State: The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State: The current state of the port. Refer to the NAS Port State for a description of the individual states.

Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class: QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about "RADIUS-assigned VLANs" here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the NAS Switch Status manually.

4-5.3 Port Status

The section provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS Port Status Configuration in the web interface:

1. Specify the port you want to check.
2. Checked “Auto-Refresh”.

Figure 4-5.3: The NAS Statistics

Parameter Description

Port State

Admin State: The port's current administrative state. Refer to “NAS Admin State” for a description of possible values.

Port State: The current state of the port. Refer to “NAS Port State” for a description of the individual states.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh, Clear): Click “Refresh” to refresh the NAS Statistics manually. You can also click “Clear” to clean up all entries.

4-6 AAA

This section shows you how to use an AAA (Authentication, Authorization, Accounting) server to provide control access to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings to use AAA servers.

4-6.1 Configuration

This section describes how to configure the AAA setting of TACACS+ or RADIUS server.

Web Interface

To configure a Common Configuration of AAA in the web interface:

1. Sets Timeout (the default is 15 seconds).
2. Sets Dead Time (the default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the web interface:

1. Selects “Enabled” in the Authorization.
2. Selects “Enabled” in the Failback to Local Authorization.
3. Selects “Enabled” in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the web interface:

1. Checks “Enabled”.
2. Specifies IP address or hostname for Radius Server.
3. Specifies authentication port for Radius Server (the default is 1812).
4. Specifies the secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the web interface:

1. Checks “Enabled”.
2. Specifies IP address or hostname for Radius Server.
3. Specifies accounting port for Radius Server (the default is 1813).
4. Specifies the secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the web interface:

1. Checks “Enabled”.
2. Specifies IP address or hostname for TACACS+ Server.
3. Specifies authentication port for TACACS+ Server (the default is 49).
4. Specifies the secret with TACACS+ Server.

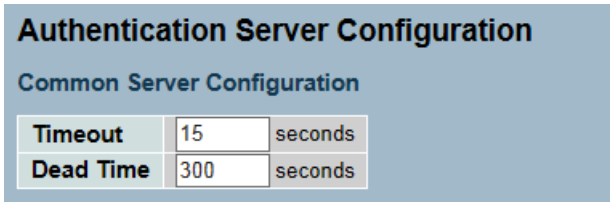


Figure 4-5.3.1: The Common Server Configuration

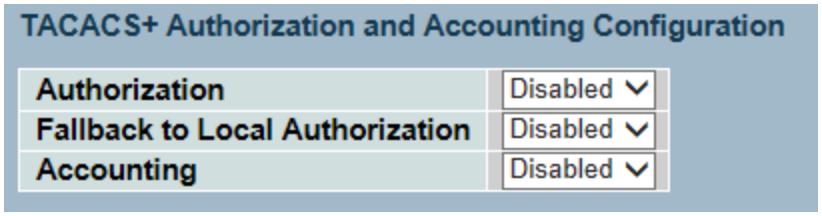


Figure 4-5.3.2: The TACACS+ Accounting Configuration

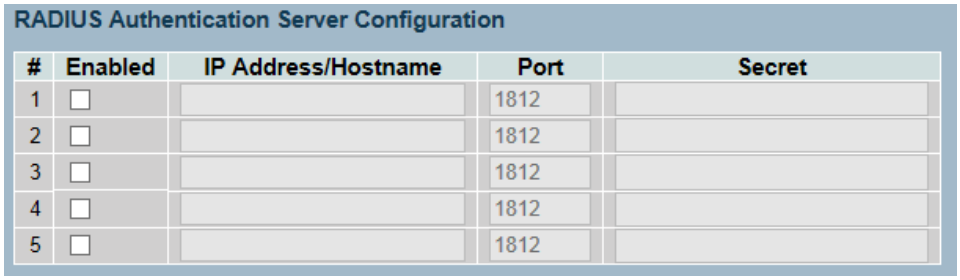


Figure 4-5.3.3: The RADIUS Configuration

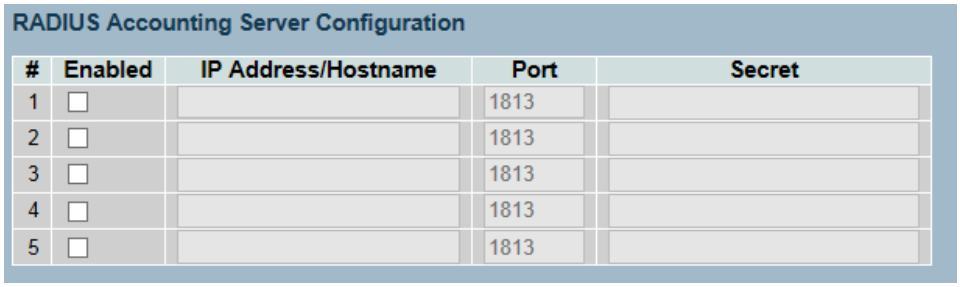


Figure 4-5.3.4: The RADIUS Accounting Configuration

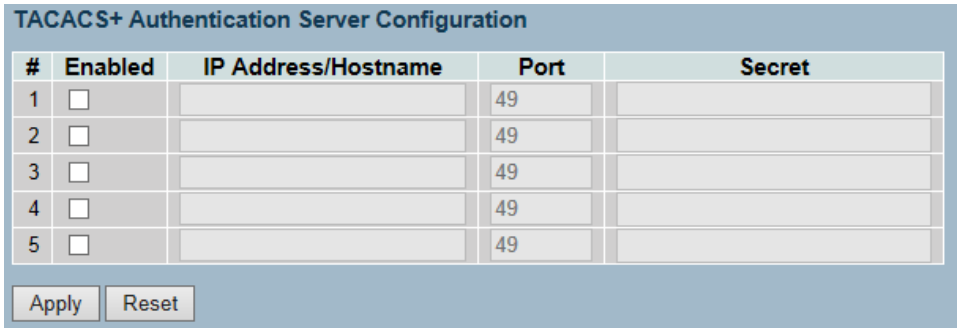


Figure 4-5.3.5: The TACACS+ Authentication Configuration

Parameter Description

Timeout: The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.

If the server does not reply within this timeframe, it will be considered as dead and continue with the next enabled server (if any).

RADIUS servers use the UDP protocol. This is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time: The dead time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the dead time to a value greater than zero (0) will enable this feature, but only if more than one server has been configured.

TACACS+ Authorization and Accounting Configuration

Authorization: Every CLI commands will be authorized by TACACS+ server when it's enabled. The authorization table on the TACACS+ server is able to configure which CLI command can pass successfully. For example, the TACACS+ server is set to accept STP command but deny VLAN command. The server will block the command related to STP which is entered by user, but it will allow the VLAN command to configure successfully when the user enters a VLAN command.

Fallback to Local Authorization: Enabled to allow the user who typed the wrong account or password to login successfully when the user account is on the local authorization list of the local switch. For example, when the user entered the wrong account or password, the TACACS+ server will refer to the account information on the local end of switch. If the account is recorded on the local switch, the user will be authorized to login with the privilege level set on the local switch.

Accounting: Enabled to record all the commands the user entered. All the log data will be recorded on the server when enabled (e.g. login time, log out time, IGMP setting, VLAN setting, and so on).

RADIUS Authentication Server Configuration

The table has one row for each RADIUS authentication server and a number of columns, which are:

#: The RADIUS authentication server number for which the configuration below applies.

Enabled: Enables the RADIUS authentication server by checking this box.

IP Address/Hostname: The IP address or hostname of the RADIUS authentication server. IP address is expressed in dotted decimal notation.

Port: The UDP port to use on the RADIUS authentication server. If the port is set to zero (0), the default port (1812) is used on the RADIUS authentication server.

Secret: The secret (up to 29 characters long) shared between the RADIUS authentication server and the switch stack.

RADIUS Accounting Server Configuration
The table has one row for each RADIUS accounting server and a number of columns, which are:

#: The RADIUS accounting server number for which the configuration below applies.

Enabled: Enables the RADIUS accounting server by checking this box.

IP Address/Hostname: The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.

Port: The UDP port to use on the RADIUS Accounting Server. If the port is set to zero (0), then the default port (1813) is used on the RADIUS Accounting Server.

Secret: The secret (up to 29 characters long) shared between the RADIUS accounting server and the switch stack.

TACACS+ Authentication Server Configuration
The table has one row for each TACACS+ authentication server and a number of columns, which are:

#: The TACACS+ authentication server number for which the configuration below applies.

Enabled: Enables the TACACS+ authentication server by checking this box.

IP Address/Hostname: The IP address or hostname of the TACACS+ authentication server. IP address is expressed in dotted decimal notation.

Port : The TCP port to use on the TACACS+ authentication server. If the port is set to zero (0), then the default port (49) is used on the TACACS+ authentication server.

Secret : The secret (up to 29 characters long) shared between the TACACS+ authentication server and the switch stack.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-6.2 Radius Overview

This section gives an overview of the RADIUS authentication and accounting servers status to ensure the function works.

Web Interface

To configure a RADIUS Overview Configuration in the web interface:

1. Checked “Auto-Refresh”.

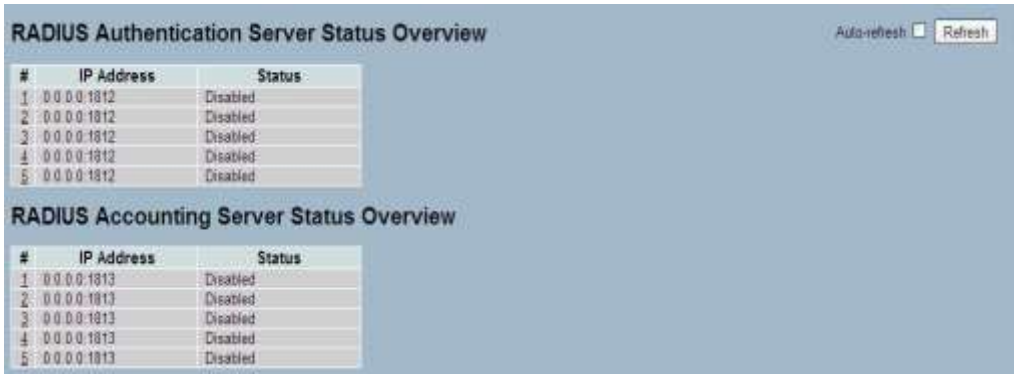


Figure 4-6.2: The RADIUS Authentication Server Status Overview

Parameter Description

#: The RADIUS server number. Click for detailed statistics of this server.

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status: The current state of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.
- **Not Ready:** The server is enabled, but the IP communication is not yet up and running.
- **Ready:** The server is enabled, the IP communication is up and running and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

#: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: The IP address and UDP port number (in <IP Address> :< UDP Port> notation) of this server.

Status: The current state of the server. This field takes one of the following values:

- **Disabled**: The server is disabled.
- **Not Ready**: The server is enabled, but the IP communication is not yet up and running.
- **Ready**: The server is enabled, the IP communication is up and running and the RADIUS module is ready to accept accounting attempts.
- **Dead (X seconds left):** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Auto-refresh: Check “Auto-Refresh” so the device can refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the RADIUS Status manually.

4-6.3 Radius Details

This section shows a detailed statistics of the RADIUS authentication and accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Web Interface

To configure a RADIUS Details Configuration in the web interface:

1. Specify the port you want to check.
2. Checked “Auto-Refresh”.

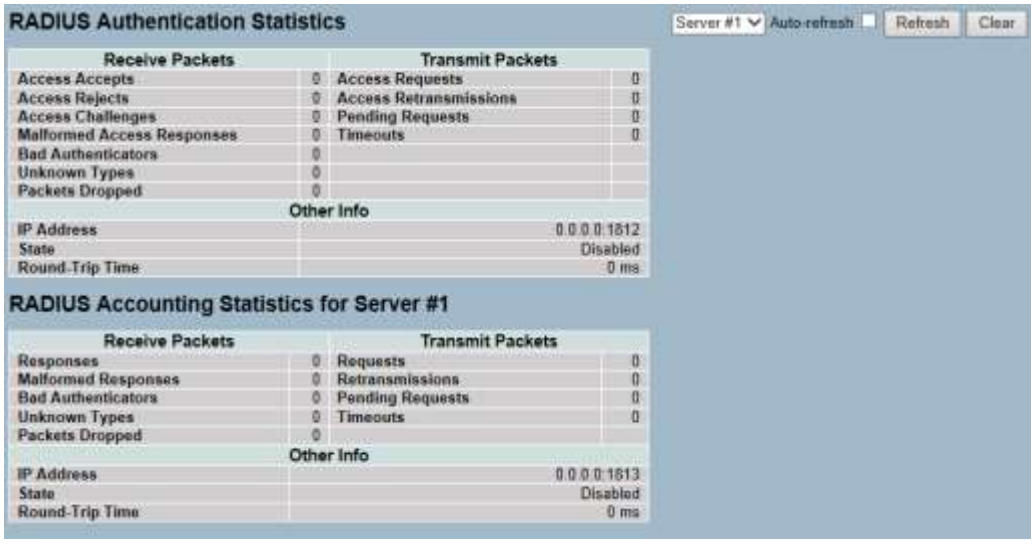


Figure 4-6.3: The RADIUS Authentication Statistics Server

Parameter Description

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators, Message Authenticator attributes, or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit, as well as, a timeout. A send to a different server is counted as a Request, as well as, a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead** (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.
Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	**Requests**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	**Retransmissions**	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	**Pending Requests**	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a response, timeout, or retransmission.
Tx	**Timeouts**	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit, as well as, a timeout. A send to a different server is counted as a request, as well as, a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but the IP communication is not yet up and running. **Ready**: The server is enabled, the IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. **Dead** (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons:

- **Auto-refresh** –Check this box to enable an automatic refresh of the page at regular intervals.
- **Refresh -** Click to refresh the page immediately.
- **Clear -** Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

4-7 Port Security

This section helps you configure the port security settings of the switch. You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses.

4-7.1 Limit Control

This section helps you configure the port security settings of the switch. You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a System Configuration of Limit Control in the web interface:

1. Select “Enabled” in the Mode of System Configuration.
2. Checked “Aging Enabled”.
3. Set “Aging Period” (The default is 3600 seconds).

To configure a Port Configuration of Limit Control in the web interface:

1. Select “Enabled” in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set “Action” (Trap, Shutdown, Trap & Shutdown.
4. Click “Apply”.

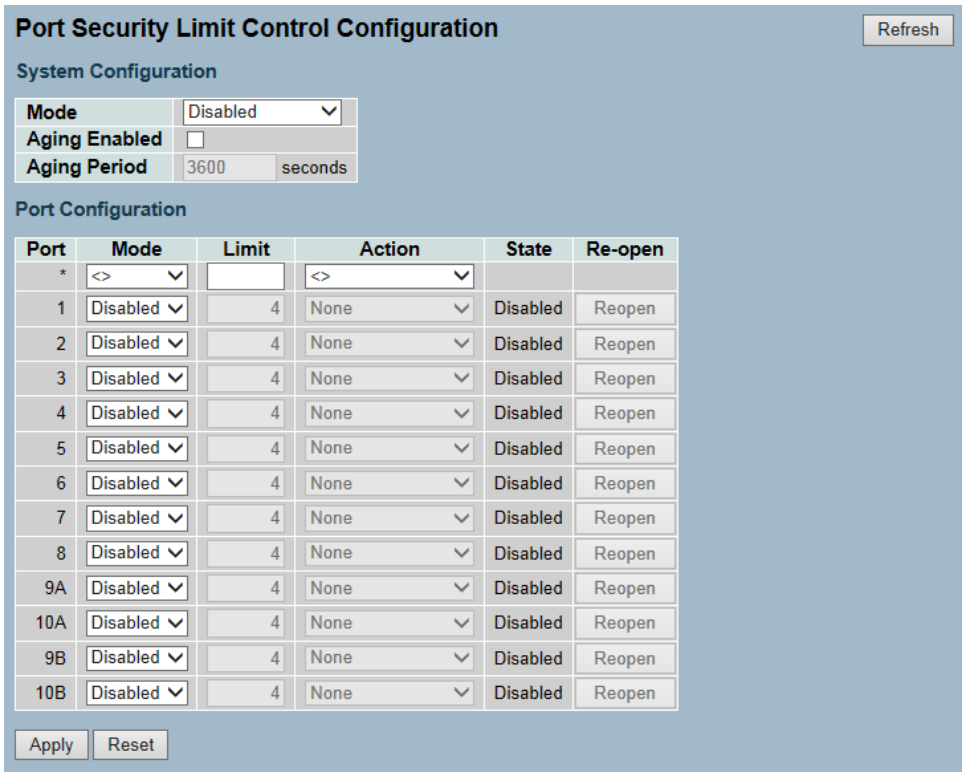


Figure 4-7.1: The Port Security Limit Control Configuration

Parameter Description

System Configuration

Mode: Indicates if “Limit Control” is globally enabled or disabled on the switchstack. If globally disabled, the other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled: If checked, secured MAC addresses are subject to aging as discussed under “Aging Period”.

Aging Period: If “Aging Enabled” is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The “Aging Period” can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Supposed an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which “Limit Control” is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now supposed that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end host gets secured. When the timer expires, the switch starts looking for frames from the end host. If such frames are not seen within the next “Aging Period”, the end host is assumed to be disconnected and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Port: The port number to which the configuration below applies.

Mode: Controls whether “Limit Control” is enabled on this port. Both this and the Global Mode must be set to “Enabled” for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The stackswitch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a port security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted if the remaining ports have already used all available MAC addresses.

Action: If the limit is reached, the switch can take one of the following actions:

- **None:** Does not allow more than the MAC addresses limit on the port, but takes no further action.
- **Trap:** If Limit + 1 MAC addresses is seen on the port, it sends a SNMP trap. If aging is disabled, only one SNMP trap will be sent. But with aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

- **Shutdown:** If Limit + 1 MAC addresses is seen on the port, it shuts down the port. This implies that all secured MAC addresses will be removed from the port and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
    1. Boot the stack or elect a new master on the switch.
    2. Disables and re-enables Limit Control on the port or the stackswitch.
    3. Click the “Reopen” button.
- **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State: This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- **Disabled:** Limit control is either globally disabled or disabled on the port.
- **Ready:** The limit is not yet reached. This can be shown for all actions.
- **Limit Reached:** Indicates that the limit is reached on this port. This state can only be shown if “Action” is set to “None” or “Trap”.
- **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if “Action” is set to “Shutdown” or “Trap & Shutdown”.

Re-open Button: If a port is shut down by this module, you may reopen it by clicking this button. It will only be enabled if this is the case. For any other methods, refer to “Shutdown” in the “Action” section.

NOTE: Clicking the reopen button causes the page to refresh and all non-committed changes will be lost.

Upper right icon (Refresh): Click “Refresh” to refresh the port security information manually.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-7.2 Switch Status

This section shows the port security status. Port Security is a module with no direct configuration. Configuration comes indirectly through other modules - the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed onto the port security module, which in turn asks all user modules whether to allow this new MAC address or to block it. In order for a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one user chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Checked “Auto-Refresh”.

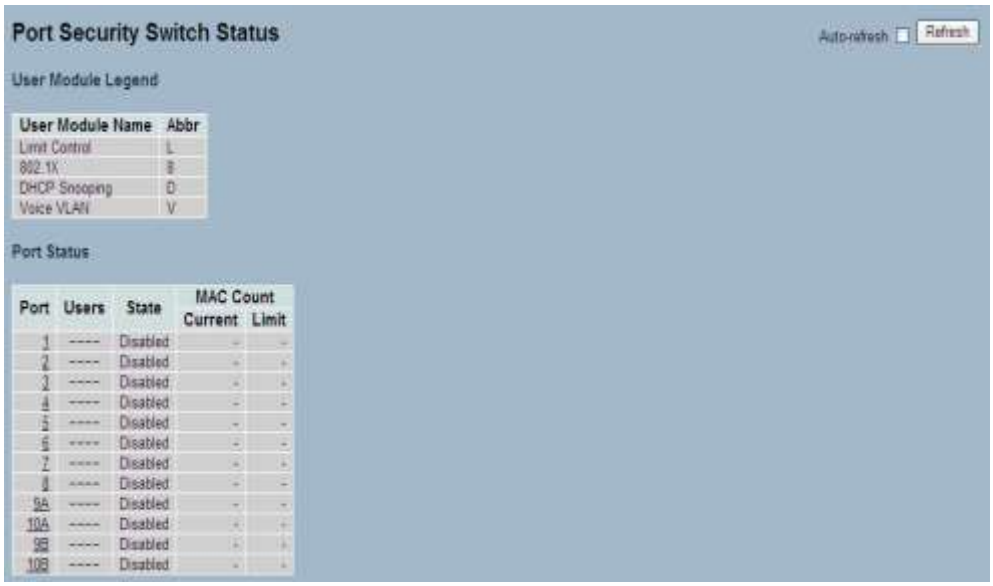


Figure 4-7.2: The Port Security Switch Status

Parameter Description

User Module Legend: The legend shows all user modules that may request port security services.

User Module Name: The full name of a module that may request port security services.

Abbr: A one-letter abbreviation of the user module. This is used in the “Users” column in the port status table.

Port Status: The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Port: The port number for which the status applies. Click the port number to see the status for this particular port.

User: Each of the user modules has a column that shows whether that module has enabled port security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State: Shows the current state of the port. It can take one of four values:

- **Disabled:** No user modules are currently using the port security service.
- **Ready:** The port security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
- **Limit Reached:** The port security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- **Shutdown:** The port security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration webpage.

MAC Count (Current, Limit) : The two columns indicate the number of currently learned MAC addresses (forwarding, as well as, blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

- If no user modules are enabled on the port, the “Current” column will show a dash (-).
- If the Limit Control user module is not enabled on the port, the limit column will show a dash (-).
- Indicates the number of currently learned MAC addresses (forwarding, as well as, blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

Auto-refresh: Check “Auto-Refresh” to refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the Port Security Switch Status information manually.

4-7.3 Port Status

This section shows the MAC addresses secured by the port security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one user chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Specify the port that you want to monitor.
2. Checked “Auto-Refresh”.

Figure 4-7.3: The Port Security Port Status

Parameter Description

MAC Address & VLAN ID: The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State: Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Shows the date and time when this MAC address was first seen on the port.

Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward and aging is enabled, the port security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Auto-refresh: Check “Auto-Refresh” to refresh the information automatically.

Upper right icon (Refresh): Click “Refresh” to refresh the Port Security Port Status information manually.

4-8 Access Management

This section helps you configure the access management table of the switch, including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN, or over the internet.

4-8.1 Configuration

This section helps you configure access management table of the switch. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Web Interface

To configure a Access Management Configuration in the web interface:

1. Select “Enabled” in the Mode of Access Management Configuration.
3. Click “Add new entry”.
4. Specify the Start IP Address, End IP Address.
5. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click “Apply”.

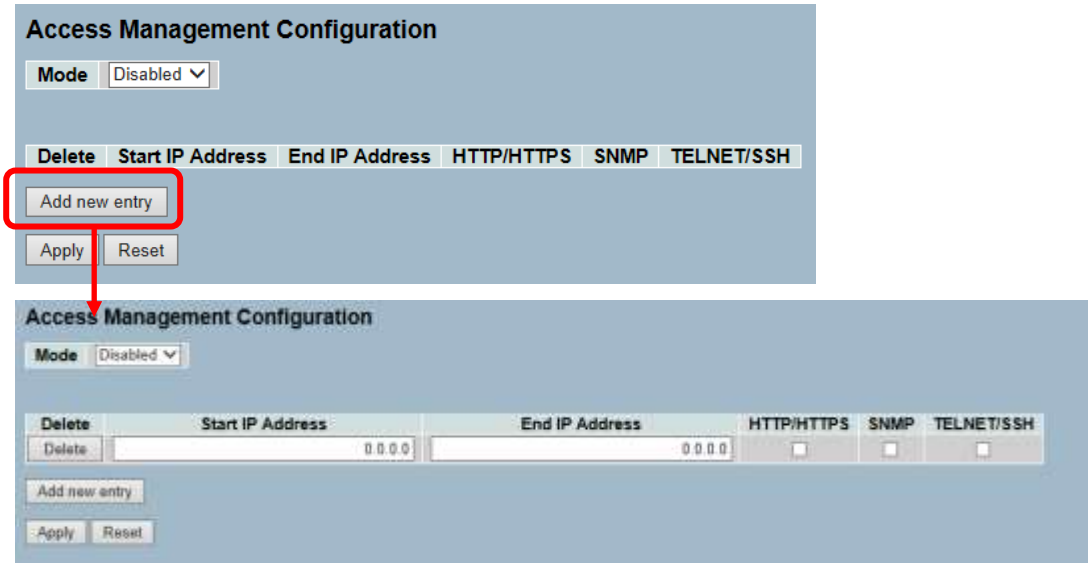


Figure 4-8.1: The Access Management Configuration

Parameter Description

Mode: Indicates the access management mode operation. Possible modes are:

- **Enabled:** Enables access management mode operation.
- **Disabled:** Disables access management mode operation.

Delete: Check to delete the entry. It will be deleted during the next save.

Start IP address: Indicates the start IP address for the access management entry.

End IP address: Indicates the end IP address for the access management entry.

HTTP/HTTPS: Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP: Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH: Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-8.2 Statistics

This section shows a detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

Web Interface

To configure an Assess Management Configuration in the web interface:

1. Checked “Auto-Refresh”.

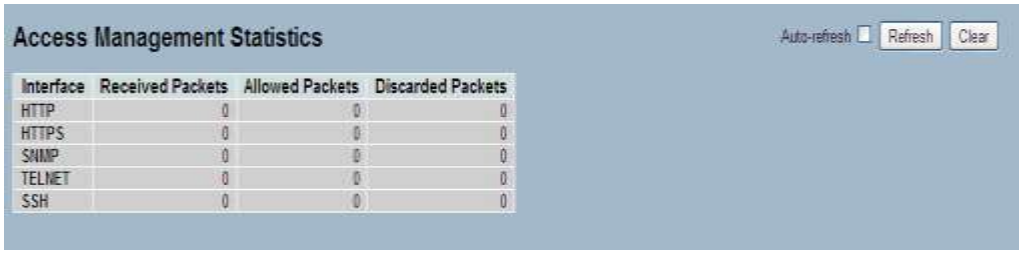


Figure 4-8.2: The Access Management Statistics

Parameter Description

Interface: The interface type through which the remote host can access the switch.

Received Packets: Number of received packets from the interface when access management mode is enabled.

Allowed Packets: Number of allowed packets from the interface when access management mode is enabled

Discarded Packets: Number of discarded packets from the interface when access management mode is enabled.

Auto-refresh: To evoke the auto-refresh icon then the device will refresh the information automatically.

Upper right icon (Refresh, Clear): Click “Refresh” to refresh the Access Management Statistics information manually. You can also click the clear button to clean up all entries.

4-9 SSH

This section shows you how to use SSH (Secure Shell) to securely access the switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure a SSH Configuration in the web interface:

1. Select “Enabled” in the Mode of SSH Configuration.
2. Click “Apply”.

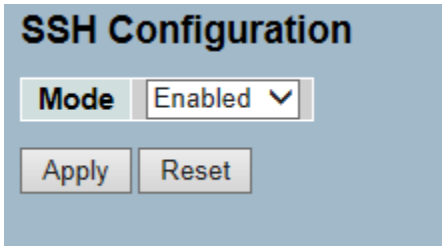


Figure 4-9.1: The SSH Configuration

Parameter Description

Mode: Indicates the SSH mode operation. Possible modes are:

- **Enabled:** Enables SSH mode operation.
- **Disabled:** Disables SSH mode operation.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-10 HTTPs

This section shows you how to use HTTPS to securely access the switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

To configure a HTTPS Configuration in the web interface:

1. Select “Enabled” in the mode of HTTPS Configuration.
2. Select “Enabled” in the Automatic Redirect of HTTPS Configuration.
3. Click “Apply”.

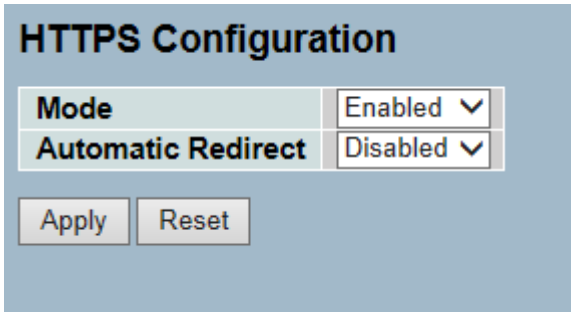


Figure 4-10.1: The HTTPS Configuration

Parameter Description

Mode: Indicates the HTTPS mode operation. Possible modes are:

- **Enabled:** Enables HTTPS mode operation.
- **Disabled:** Disables HTTPS mode operation.

Automatic Redirect: Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

- **Enabled:** Enables HTTPS redirect mode operation.
- **Disabled:** Disables HTTPS redirect mode operation.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

4-11 Auth Method

This page shows how to authenticate a user when he logs into the switchstack, via one of the management client interfaces.

Web Interface

To configure a Authentication Method Configuration in the web interface:

1. Specify the Client (Console, Telnet, SSH, Web) which you want to monitor.
2. Specify the Authentication Method (None, Local, Radius, TACACS+).
3. Checked “Fallback”.
4. Click “Apply”.

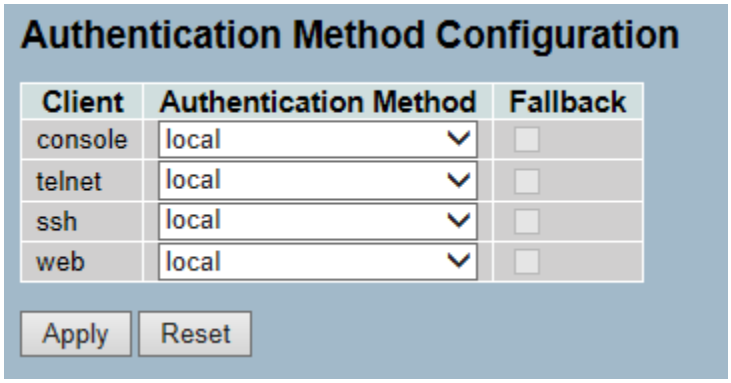


Figure 4-11.1: The HTTPS Configuration

Parameter Description

Client: The management client for which the configuration below applies.

Authentication Method: Authentication method can be set to one of the following values:

- **None**: Authentication is disabled and login is not possible.
- **Local**: Uses the local user database on the switch stack for authentication.
- **Radius**: Uses a remote RADIUS server for authentication.
- **TACACS**+: Uses a remote TACACS+ server for authentication.

Fallback: Enables the fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the Authentication Method is set to a value other than “None” or “Local”.

Buttons:

- **Apply** – Click “Apply” to save changes.
- **Reset-** Click “Reset” to undo any changes made locally and revert to previously saved values.

Chapter 5: Maintenance

Chapter 5 describes all of the switch's maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

5-1 Restart

This section describes how to restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the web interface:

1. Click "Restart Device".
2. Click "Yes".

Figure 5-1.1: The Restart Device

Restart Device: You can restart the stack switch on this page. After restarting, the stack switch will boot normally.

Buttons:

- **Yes** – Click "Yes" to restart the device.
- **No-** Click "No" to undo any restart action.

5-2 Firmware

This section describes how to upgrade firmware for the device. The switch can be enhanced with more value-added functions by installing firmware upgrades.

5-2.1 Firmware Upgrade

This section describes how to upgrade firmware for the device. The switch can be enhanced with more value-added functions by installing firmware upgrades.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Click “Browse” to select the firmware for your device.
2. Click “Upload”.

Figure 5-2.1: The Firmware update

Parameter Description

Browse: Click the “Browse...” button to search the firmware URL and filename.

Upload: Click the “Upload” button, then the switch will start to upload the firmware from firmware stored location PC or Server.

NOTE: This page facilitates an update of the firmware to control the stack switch. Uploading software will update all managed switches in the stack to the location of a software image. After the software image is uploaded, the firmware update is initiated. After about a minute, the firmware is updated and all managed switches in the stack restart. The switch restarts.

WARNING: While the firmware is being updated, web access appears to be dysfunctional. The front LED flashes Green/Off with a frequency of 10 Hz, while the firmware update is in progress. Do not restart or power off the device at this time, or the switch may fail to function afterwards.

5-2.2 Firmware Selection

The switch supports dual image for firmware redundancy purpose. You can select what firmware image for your device: start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

Web Interface

To configure a firmware selection in the web interface:

1. Click “Activate Alternate Image”.
2. Click “Yes” to complete firmware selection.

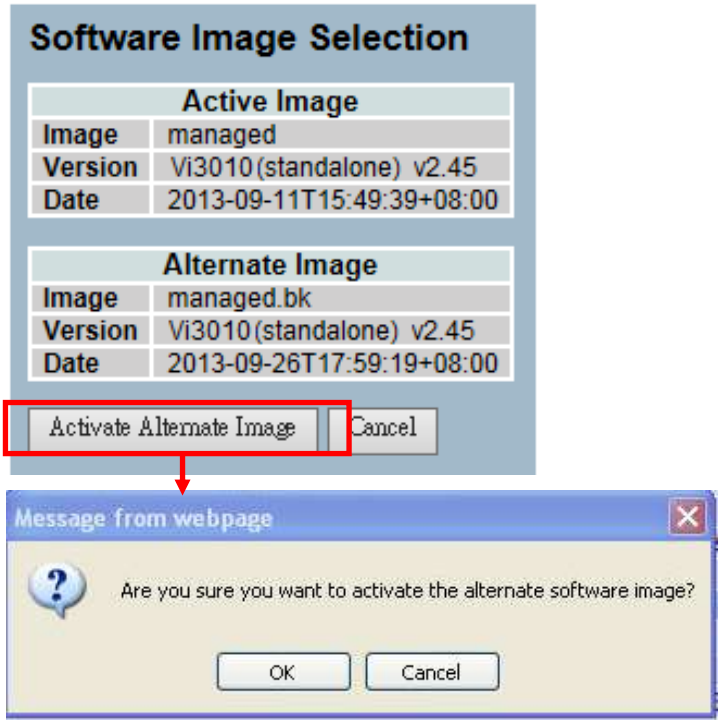


Figure 5-2.2: The Firmware Selection

Parameter Description

Activate Alternate Image: Click to use the alternate image. This button may be disabled, depending on the system state.

Cancel: Cancel activating the backup image. Navigates away from this page.

Image: The flash index name of the firmware image. The name of primary (preferred) image is “image”. The alternate image is named “image.bk”.

Version: The version of the firmware image.

Date: The date when the firmware was produced.

NOTE:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the “Activate Alternate Image” button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or manually intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

5-3 Save/Restore

This section describes how to save and restore the switch configuration including Reset to Factory Defaults, Save Start, Save Users, and Restore Users for any maintenance needs.

5-3.1 Factory Defaults

This section describes how to reset the switch configuration to factory defaults. Any configuration files or scripts will recover to factory default values.

Web Interface

To configure a Factory Defaults Configuration in the web interface:

1. Click “Factory Defaults”.
2. Click “Yes”.

Factory Defaults
Are you sure you want to reset the configuration to Factory Defaults?
Restore Default Configuration without changing current IP address
Yes
No

Figure 5-3.1: The Factory Defaults

Parameter Description

Buttons:

- **Yes** – Click to “Yes” button to reset the configuration to factory defaults.
- **No-** Click “No” to return to the port state page without resetting the configuration.

5-3.2 Save Start

This section describes how to save the Switch Start Configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save Start Configuration in the web interface:

1. Click “Save Start”.
2. Click “Yes”.

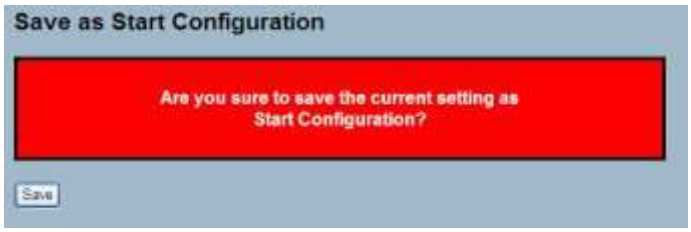


Figure 5-3.2: “Save Start” configuration

Parameter Description

Buttons:

- **Save** – Click the “Save” button to save current setting as Start Configuration.

5-3.3 Save User

This section describes how to save users information. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save User Configuration in the web interface:

1. Click “Save User”.
2. Click “Yes”.

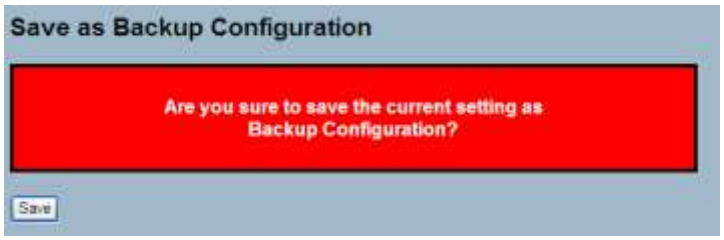


Figure 5-3.3: “Save” as Backup Configuration

Parameter Description

Buttons:

- **Save –** Click the “Save” button to save current setting as Backup Configuration.

5-3.4 Restore User

This section describes how to restore the users information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a Restore User Configuration in the web interface:

1. Click “Restore User”.
2. Click “Yes”.

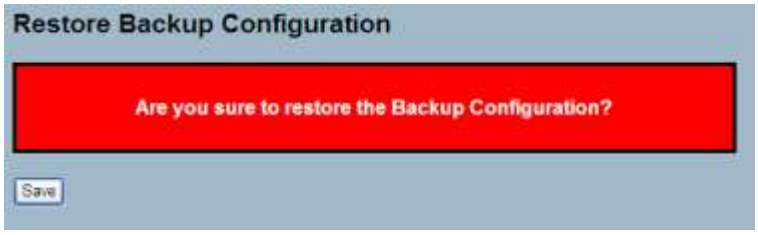


Figure 5-3.4: The Restore the Backup Configuration

Parameter Description

Buttons:

- **Save –** Click the “Save” button to restore the Backup Configuration to the switch.

5-4 Export/Import

This section describes how to export and import the switch configuration. Any current configuration files will be exported as XML format.

5-4.1 Export Config

This section describes to export the swith configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure the Export Config Configuration in the web interface:

1. Click “Save configuration”.
2. Save the file in your device.

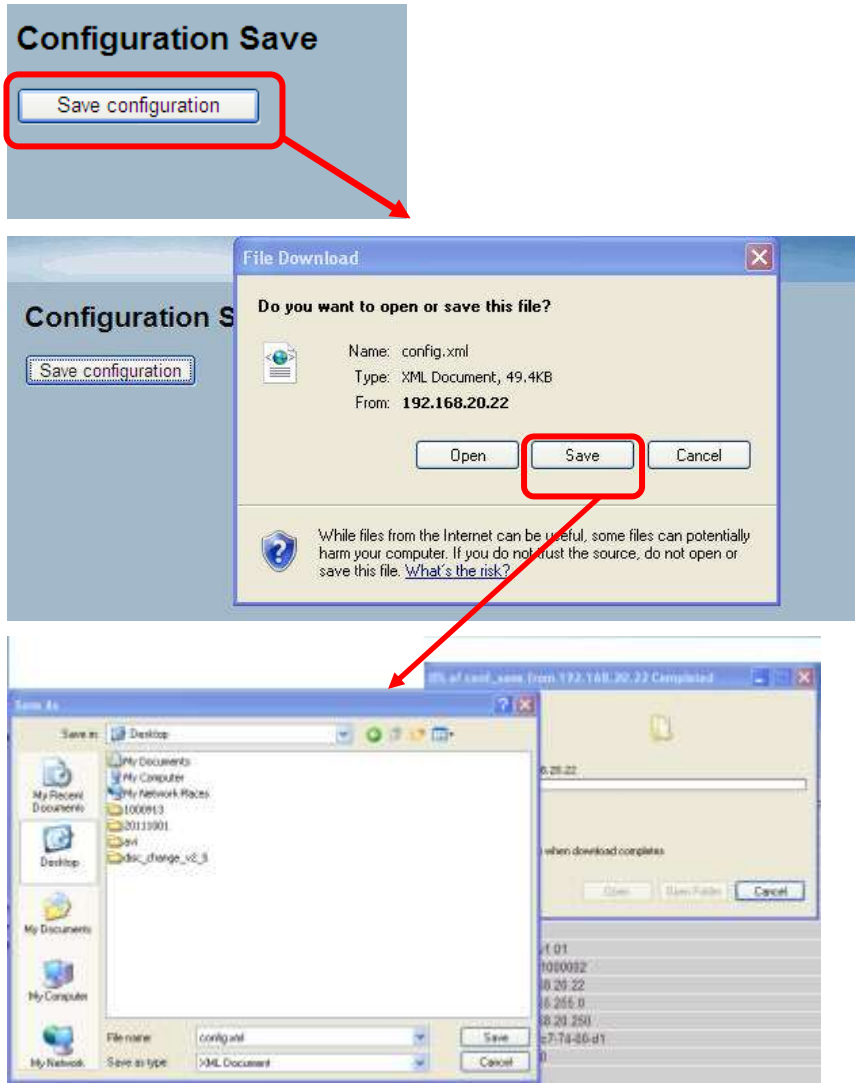

Configuration Save
Save configuration
File Download
Do you want to open or save this file?
Name: config.xml
Type: XML Document, 49.4KB
From: 192.168.20.22
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 5-4.1: The Restore the Backup Configuration

Parameter Description

Save – Click the “Save” button to store the configuration to the PC or server.

5-4.2 Import Config

This section describes to export the switch configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an Import Config Configuration in the web interface:

1. Click “Browse” to select the config file in your device.
2. Click “Upload”.

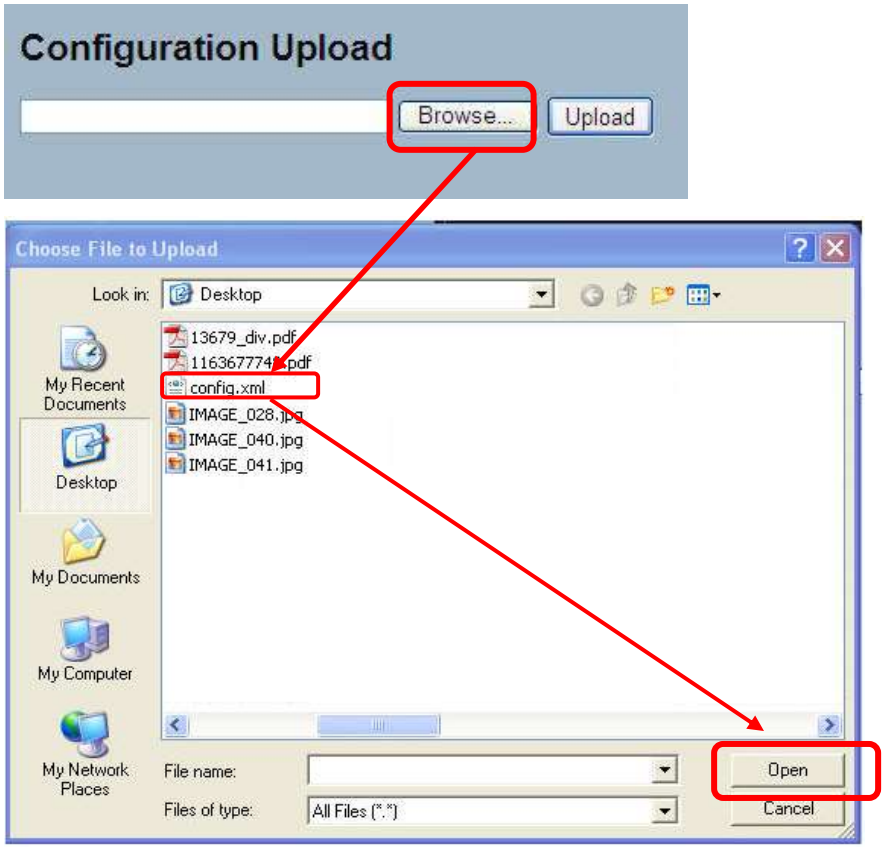


Figure 5-4.2: The Import Config

Parameter Description

Browse: Click the “Browse...” button to search the configuration URL and filename.

Upload: Click the “Upload” button, and then the switch will start to upload the configuration to the PC or server.

5-5 Diagnostics

This section provides a set of basic system diagnosis. It indicates whether the system is healthy or if it needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

5-5.1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the web interface:

1. Specify ICMP PING IP address.
2. Specify ICMP PING size.
3. Click “Start”.

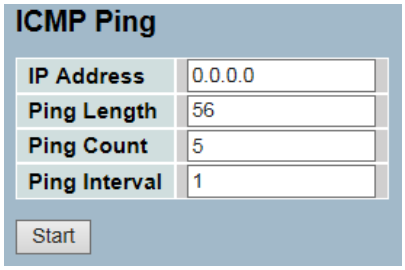


Figure 5-5.1: The ICMP Ping

Parameter Description

IP Address: To set the IP Address of device what you want to ping it.

Ping Length: The payload size of the ICMP packet. The values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. The values range from 1 time to 60 times.

Ping Interval: The interval of the ICMPv6 packet. The values range from 0 second to 30 seconds.

Start: Click the “Start” button, then the switch will start to ping the device using ICMP packet size what set on the switch.

After you press start, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received or until a timeout occurs.

PING6 server ::10.10.132.20

64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

5-5.2 Ping6

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify ICMPv6 PING IP Address.
2. Specify ICMPv6 PING Size.
3. Click “Start”.

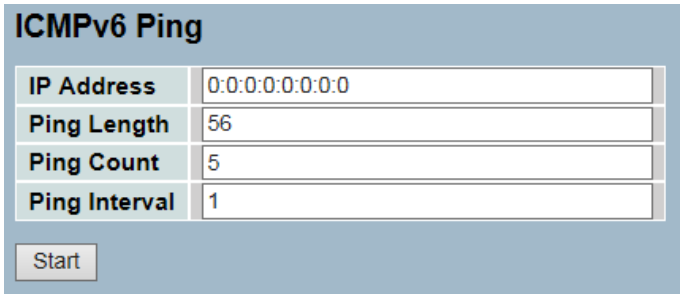


Figure 5-5.2: The ICMPv6 Ping

Parameter Description

IP Address: The destination IP Address with IPv6.

Ping Length: The payload size of the ICMPv6 packet. The values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMPv6 packet. The values range from 1 time to 60 times.

Ping Interval: The interval of the ICMPv6 packet. The values range from 0 second to 30 seconds.

Start: Click the “Start” button, then the switch will start to ping the device using ICMPv6 packet size what set on the switch.

After you press start, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received or until a timeout occurs.

You can configure the following properties of the issued ICMP packets:

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

5-5.3 VeriPHY

This section is used to run the VeriPHY Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take up to 15 seconds. When completed, the page refreshes automatically and the cable diagnostics results will be viewable in the cable status table. Note that VeriPHY is only accurate for cables that are 7 -140 meters in length. 10 and 100 Mbps ports will be linked down while VeriPHY is running. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web Interface

To configure a VeriPHY Cable Diagnostics Configuration in the web interface:

1. Specify the port you want to check.
2. Click “Start”.

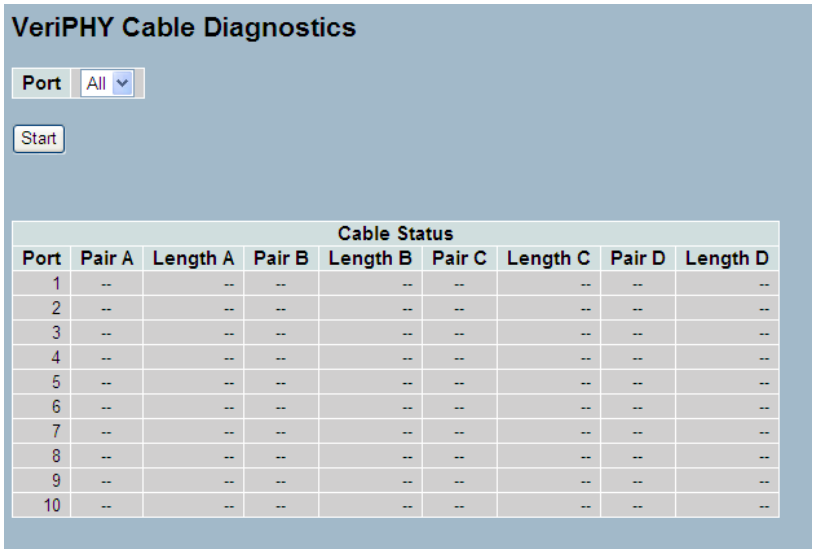

VeriPHY Cable Diagnostics
Port
All
Start
Cable Status
Port Pair A Length A Pair B Length B Pair C Length C Pair D Length D
1 -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- --
7 -- -- -- -- -- -- -- --
8 -- -- -- -- -- -- -- --
9 -- -- -- -- -- -- -- --
10 -- -- -- -- -- -- -- --

Figure 5-5.3: The VeriPHY

Parameter Description

Port: The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status:

- **Port**: Port number.
- **Pair**: The status of the cable pair.
- **Length**: The length (in meters) of the cable pair.

5-6 Battery Replacement

It is recommended that only qualified service personnel replace the internal battery.

CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Glossary of Web-Based Management

A

ACE: ACE is an acronym for Access Control Entry. It describes the access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (Permit and Deny). The ACE also contains different detailed parameter options that are available for individual application.

ACL: ACL is an acronym for Access Control List. It is the list of ACEs. It contains access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex (e.g. when the ACEs are prioritized for the various situation). In networking, the ACL refers to a list of service ports or network services that are available on a host or server. Each has a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic (they are similar to firewalls).

There are 3 webpages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs from highest (top) to lowest (bottom). The default the table is empty. An ingress frame will only get a hit on one ACE, even though there are other matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, 1 ingress port, or any ingress port (the whole switch). If an ACE policy is created, then that policy can be associated with a group of ports under the "Ports" webpage. There are a number of parameters that can be configured with an ACE. Read the webpage help text to get further information. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic policy is created under the "Access Control List" page. You can also set up specific traffic properties (Action, Rate Limiter, Port Copy and so on) for each ingress port. They will only apply if the frame gets past the ACE matching process without getting matched. In that case, a counter associated with that port is incremented. See the webpage help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, ranging from 1-1024K packets per seconds. Under the "Ports" and "Access Control List" webpages, you can assign a rate limiter ID to the ACE(s) or ingress port(s).

AES: AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which replaces DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS: APS is an acronym for Automatic Protection Switching. This protocol is used to make sure that switching is done bidirectional at the two ends of a protection group, as defined in G.8031.

Aggregation: Aggregation uses multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also Port Aggregation, Link Aggregation).

ARP: ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request that contains the Internet address of the desired destination system.

ARP Inspection: ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation: Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC: CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM: CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP: CDP is an acronym for Cisco Discovery Protocol.

D

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES: DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.

DHCP: DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique. For example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, the IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay: DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information to a DHCP request packet when forwarding client DHCP packets to a DHCP server, and removing specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. The option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length. The format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes that represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (In standalone switch, it always equal 0. In stackable switch, it means switch ID). The parameter of "port_no" is the fourth byte that represents the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping: DHCP Snooping is used to block intruders on the untrusted ports of the switch device. The intruder gets blocked when it tries to inject a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS: DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name “www.example.com” might translate to 192.168.0.1.

DoS: DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, the attacker may be able to prevent network users from accessing email, web sites, online accounts (e.g. banking accounts and more), or other services that rely on the affected computer.

Dotted Decimal Notation: Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w. The values x, y, z, and w are decimal numbers between 0 and 255.

DSCP: DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE: EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS: EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type: Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP: FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP). It provides file writing and reading. It also provides directory service and security features.

Fast Leave: Multicast Snooping Fast Leave process allows the switch to remove an interface from the forwarding-table entry, without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP: HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions the web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, it sends a HTTP command to the web server. It directs the web server to fetch and transmit the requested webpage. The other main standard that controls how the World Wide Web works is HTML, which covers how webpages are formatted and displayed.

Any web server machine contains and serves a HTTP daemon, a program that is designed to wait for HTTP requests and process them when they arrive. The web browser is a HTTP client that sends requests to server machines. A HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). A HTTP server listening on that port waits for the client to send a request message.

HTTPS: HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication, such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub layer under its regular HTTP application layering (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP). SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP: ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges, such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE802.1X: IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port to establish a point-to-point connection or to prevent access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP: IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming. It allows for more efficient use of resources when supporting these uses.

IGMP Querier: A router sends IGMP Query messages to a particular link. This router is called the Querier.

IP: IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address. This IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4. IPv4 has 32-bits Internet Protocol addresses, allowing for an excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC: IPMC is an acronym for IP MultiCast.

IP Source Guard: IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports, by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP: LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol allows bundling of several physical ports together to form a single logical port.

LLC: The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), and 1 or 2 bytes Control field followed by LLC information.

LLDP: LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations that are attached to an IEEE 802 LAN to advertise to other stations attached to the same IEEE 802 LAN. The major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol. For example, the Simple Network Management Protocol (SNMP).

LLDP-MED: LLDP-MED is an extension of IEEE 802.1ab. It is defined by the telecommunication industry association (TIA-1057).

LOC: LOC is an acronym for Loss Of Connectivity. It is detected by a MEP and indicates a lost connectivity in the network. It can be used as switch criteria by EPS.

M

Mac Table: Switching of frames is based upon the DMAC address contained in the frame. The switch builds a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table, if no frame with the corresponding SMAC address has been seen after a configurable age time.

MEP: MEP is an acronym for Maintenance Entity Endpoint. It is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5: MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring: For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. In this context, mirroring a frame is the same as copying the frame.

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD: MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, such as IGMP is used in IPv4. The protocol is embedded in ICMPv6, instead of using a separate protocol.

MVR: Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network. Instead, the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS: NAS is an acronym for Network Access Server. The NAS acts as a gateway to the guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource to ask whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS: NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN). It is not supported on a Wide Area Network (WAN).

The NetBIOS gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name. It provides the session and transports services described in the Open Systems Interconnection (OSI) model.

NFS: NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network to provide authorized users continuous access to them. This means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP: NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM: OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs: A LLDP frame contains multiple TLVs. For some TLVs, it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.

OUI: OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address, which forms the first 24 bits of a MAC address.

P

PCP: PCP is an acronym for Priority Code Point. It is a 3-bit field that stores the priority level for the 802.1Q frame. It is also known as “User Priority”.

PD: PD is an acronym for Powered Device. In a PoE system, the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY: PHY is an abbreviation for Physical Interface Transceiver. It is the device that implements the Ethernet physical layer (IEEE-802.3).

PING: PING is a program that sends a series of packets over a network or the Internet to a specific computer, in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

PING uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE: PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. For example, it could be used for powering IP telephones, wireless LAN access points, and other equipment where it would be difficult or expensive to connect the equipment to main power supply.

Policer: A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Private VLAN: In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP: PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

QCE: QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL: QCL is an acronym for QoS Control List. It is the list of QCEs that contains QoS control entries classified to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL: QL in SyncE is the Quality Level of a given clock source. This is received on a port in a SSM to indicate the quality of the clock received in the port.

QoS: QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP: RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS: RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI: RDI is an acronym for Remote Defect Indication. It is a OAM functionality used by a MEP to indicate defect detected to the remote peer MEP.

RSTP: In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time, being backwards-compatible with STP.

S

SHA: SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper: A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP: SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP: The Sub Network Access Protocol (SNAP) is a mechanism for multiplexing on networks using IEEE 802.2 LLC. More protocols can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values. It also supports vendor-private protocol identifier.

SNMP: SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows diverse network objects to participate in network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP: SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT: Stack Protocol uses Routing Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack, as well as, election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID: Service Set Identifier is a name used to identify the particular 802.11 wireless LANs that a user wants to attach. A client device will receive broadcast messages from all access points within range to advertise their SSIDs. It can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (Wikipedia).

SSH: SSH is an acronym for Secure Shell. It is a network protocol that allows data to be exchanged, using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM: SSM is an abbreviation for Synchronization Status Message. It is contains a QL indication.

STP: Spanning Tree Protocol is an OSI layer-2 protocol, which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch IDs: Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display in front of the switch. It is used widely in the web pages and CLI commands.

SyncE: SyncE is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. It should not be confused with real time clock synchronized (IEEE 1588).

T

TACACS+: TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol that provides access control for routers, network access servers and other networked computing devices, via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority: Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP: TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

TCP protocol guarantees reliable and in-order delivery of data from the sender to the receiver. It distinguishes data for multiple connections by concurrent applications (e.g. Web server and e-mail server) running on the same host.

The applications on network hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol. This means that a connection is established and maintained until the messages have been exchanged by the application programs at each end. TCP is responsible for ensuring that a message is divided into the packets that IP manages. It also reassembles the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET: TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP). It provides a virtual connection between TELNET server and TELNET client.

TELNET lets the client control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client can enter commands through the Telnet program, just as if they were entering commands directly on the server console.

TFTP: TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP). It provides file writing and reading. It does not provide directory service and security features.

U

UDP: UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP), that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams. UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and as an option, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications (such as IPTV), Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority: User Priority is a 3-bit field that stores the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN: Virtual LAN is a method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID: VLAN ID is a 12-bit field that specifies which VLAN the frame belongs to.

Voice VLAN: Voice VLAN is VLAN configured specifically for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data to ensure the transmission priority of voice traffic and voice quality.

Contact Information

Vigitron, Inc.

7810 Trade Street, Suite 100
San Diego, CA 92121
support@vigitron.com
Tel: (858) 484-5209
Fax: (858) 484-1205
www.vigitron.com